ASPJ Air & Space Power Journal

Vol. 34, Issue 4 Winter 2020

Air Force meshes Info-War capabilities

US fires up "all government" war on election cyberthreats

State-sponsored cyberattacks on banks on the rise

Tail spotters track B-2 deployment in near real-time using open source tools

US authorities investigating if recently published emails are tied to Russian disinformation

Chinese hackers suspected in cyber-espionage operation

North Korea debuts new propaganda "vloggers" to attract foreign viewers

Iran targeting US state voter rolls and spreading election propaganda, officials say

US planes drop leaflets over Iraq

US seizes Iranian domains used for propaganda

ASPJ Air & Space Power Journal

Chief of Staff, US Air Force
Gen Charles Q. Brown, Jr., USAF

Chief of Space Operations, US Space Force
Gen John W. Raymond, USSF

Commander, Air Education and Training Command
Lt Gen Marshall B. Webb, USAF

Commander and President, Air University
Lt Gen James B. Hecker, USAF

Director, Academic Services
Dr. Mehmed Ali

Acting Director, Air University Press
Maj Richard T. Harrison, USAF

Editorial Staff

Maj Richard T. Harrison, USAF, *Editor*
Capt Jayson M. Warren, USAF, Guest Editor
Randy Roughton, *Content Editor*
Daniel M. Armstrong, *Illustrator*
Tim Thomas, *Illustrator*
Megan N. Hoehn, *Print Specialist*

Air & Space Power Journal
600 Chennault Circle
Maxwell AFB AL 36112-6010
e-mail: aspj@au.af.edu

Visit *Air & Space Power Journal* online at https://www.airuniversity.af.edu/ASPJ/.

The *Air & Space Power Journal* (ISSN 1554-2505), Air Force Recurring Publication 10-1, published quarterly in both online and printed editions, is the professional journal of the Department of the Air Force. It is designed to serve as an open forum for the presentation and stimulation of innovative thinking on military doctrine, strategy, force structure, readiness, and other matters of national defense. The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, the Department of the Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

In this edition, articles not bearing a copyright notice may be reproduced in whole or in part without permission. Articles bearing a copyright notice may be reproduced for any US government purpose without permission. If they are reproduced, the *Air & Space Power Journal* requests a courtesy line. To obtain permission to reproduce material bearing a copyright notice for other than US government purposes, contact the author of the material rather than the *Air & Space Power Journal*.

https://www.af.mil/ https://www.spaceforce.mil/ https://www.aetc.af.mil/ https://www.airuniversity.af.edu/

VOL. 34 NO. 4 WINTER 2020

FOREWORD

4 **Foreword**
Lt Gen Mary F. O'Brien, USAF

SENIOR LEADER PERSPECTIVES

5 **Achieving Convergence in the Information Environment**
Revising the Air Component Structure
Brig Gen George M. Reynolds, USAF

15 **Command and Control of Operations in the Information Environment**
Leading with Information in Operational Planning, Execution, and Assessment
Sandeep S. Mulgund, PhD
Gen Mark D. Kelly, USAF

FEATURES

27 **Restructuring Information Warfare in the United States**
Shaping the Narrative of the Future
Capt Anthony J. Eastin, USAF
1st Lt Patrick G. Franck, USAF

40 **Information Warfare**
Tuning Our Instruments to Overcome Barriers to Battlefield Harmony
Col Nathaniel Huston, USAF
Capt Keegan Newton, USAF
Capt John Runge, USAF

54 **Empowering the Information Warrior**
Unlocking the Latent Value of this Strategic Asset
Jay Fudemberg
Lt Col Robert D. Folker Jr., USAF, Retired

75 **Not All Wars Are Violent**
Identifying Faulty Assumptions for the Information War
Capt Jayson Warren, USAF

VIEWS

91 **The Spectrum of Cyber Attack**
Maj David Musielewicz, USAF

101 **Information Warfare and Joint All-Domain Operations**
A Primer for Integrating and Prioritizing Data Requirements
Lt Col Bradley M. Pirolo, USAF

BOOK REVIEW

108 ***Military Strategy in the 21st Century: People, Connectivity, and Competition***
by Charles Cleveland, Benjamin Jensen, Susan Bryant, and Arnel David
Reviewed by Lt Col Benjamin L. Carroll, USAF

Air & Space Power Journal Reviewers

Filomeno Arenas, PhD
USAF Air Command and Staff College

Bruce Bechtol, PhD
Angelo State University

Kendall K. Brown, PhD
NASA Marshall Space Flight Center

Anthony C. Cain, PhD
Wetumpka, Alabama

Norman C. Capshaw, PhD
Military Sealift Command Washington Navy Yard, District of Columbia

Christopher T. Colliver, PhD
Wright-Patterson AFB, Ohio

Chad Dacus, PhD
USAF Cyber College

Lt Col Andrew Dulin, USAF
16th AF Information Operations Director of Staff

Maj Gen Charles J. Dunlap Jr., USAF, Retired
Duke University

Lt Col Derrill T. Goldizen, PhD, USAF, Retired
Naval War College

Col Jeffrey J. Gomes, USAF
Sixteenth Air Force/J39

Col Mike Guillot, USAF, Retired
Editor, Strategic Studies Quarterly

Col Dale L. Hayden, PhD, USAF, Retired
Birmingham, Alabama

John M. Hinck, PhD
USAF Air War College

Brig Gen S. Clinton Hinote, USAF
Air Force Warfighting Integration Capability HAF/AJA, Pentagon

Thomas Hughes, PhD
USAF School of Advanced Air and Space Studies

Lt Col J. P. Hunerwadel, USAF, Retired
Curtis E. LeMay Center for Doctrine Development and Education

Tom Keaney, PhD
Senior Fellow, Merrill Center at the School of Advanced International Studies

Col Merrick E. Krause, USAF, Retired
Executive Director, Resource Management and Planning Board of Veterans' Appeals, Veteran's Affairs

Benjamin S. Lambeth, PhD
Center for Strategic and Budgetary Assessments

Maj James Maher, USAF
US Air Force Academy Department of Computer and Cyber Sciences

Rémy M. Mauduit
Montgomery, Alabama

Col Phillip S. Meilinger, USAF, Retired
West Chicago, Illinois

Richard R. Muller, PhD
USAF School of Advanced Air and Space Studies

Lt Col Jason M. Newcomer, DBA, USAF
USAF Air Command and Staff College

Col Robert Owen, USAF, Retired
Embry-Riddle Aeronautical University

Lt Col Brian S. Pinkston, USAF, MC, SFS
Air Force Review Board Agency

Maj Gen John E. Shaw, USAF
Headquarters Air Force Space Command A5/8/9 Peterson AFB, Colorado

Col Richard Szafranski, USAF, Retired
Isle of Palms, South Carolina

Lt Col Michael Tate, USAF, Retired
USAF Air University

Lt Col Edward B. Tomme, PhD, USAF, Retired
CyberSpace Operations Consulting

Lt Col David A. Umphress, PhD, USAFR, Retired
Auburn University

CMSgt Michael J. Young, USAF, Retired
Montgomery, Alabama

Xiaoming Zhang, PhD
USAF Air War College

Brent A. Ziarnick, PhD
USAF Air Command and Staff College

FOREWORD

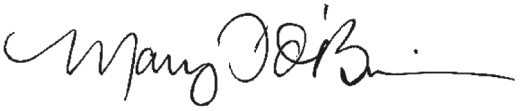
Our Air Force must accelerate change to control and exploit the air domain to the standard the nation expects and requires from us. If we don't change—if we fail to adapt—we risk losing the certainty with which we have defended our national interest for decades.

Accelerate Change or Lose—Gen CQ Brown, 22nd USAF chief of staff

We are engaged in strategic competition in the information space; *Accelerating Change* in information warfare (IW) is an imperative we ignore at our peril. Our great power competitors are already engaged—IW concepts are engrained in their strategic doctrine, reflected in organizational changes and embedded in their training at all levels. China and Russia are maneuvering every day in the IW space, and without swift whole-of-government action, we may find ourselves unable to contest them.

In order to compete effectively in the IW space, we must understand our constraints—strategic culture, organizational seams, and investment trades are only a few examples. In turn, we require better insight into how we could constrain our adversaries. During competition, IW success is often, but not always, measured in small increments that accumulate to strategic advantage over extended periods. If we fly an aircraft along a new route on a given day, does it have the anticipated effect…or are we causing unintended consequences? If we block an access vector, will the adversary shift to an approach we are prepared to secure, or one we cannot defend? Do we know enough about the adversary to draw them into a decision cycle of our choosing? How can we be certain we are pulling the right informational levers at the right time to encourage (or discourage) adversary behaviors?

Information warfare may be the deciding factor in strategic competition. The collection of articles in this information warfare edition of the *Air & Space Power Journal* proves our Airmen are more than ready to contribute their good ideas. Whether it's addressing the overdue need for a standardized IW lexicon, outlining training requirements for our information warriors of the future, or designing campaigns, exercises and operations around shaping adversary perceptions and behaviors, our Airmen are ready to seize the initiative and revolutionize IW operations!



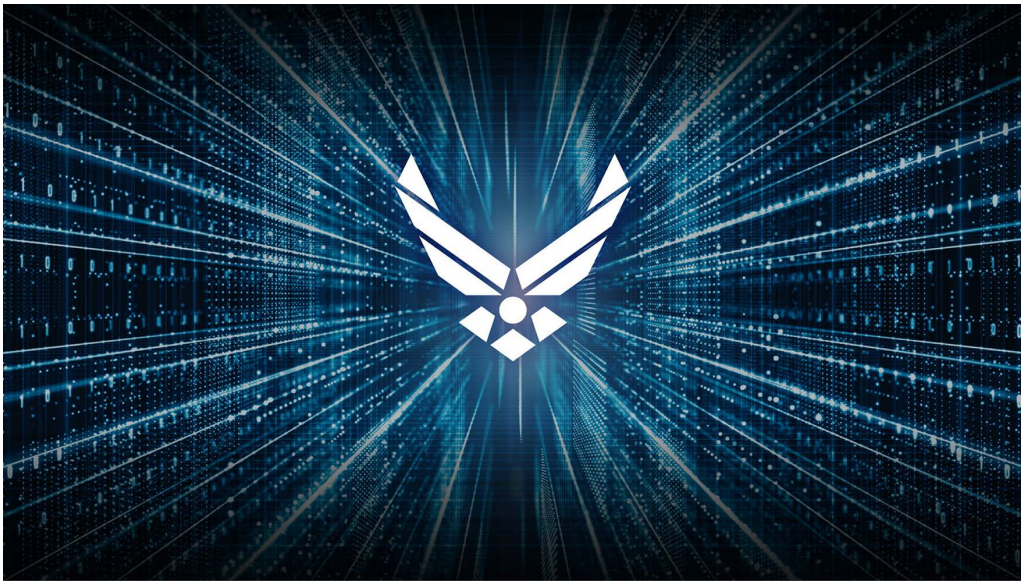
Lt Gen Mary F. O'Brien
Deputy chief of staff, Headquarters USAF,
Intelligence, Surveillance, Reconnaissance
and Cyber Effects Operations

SENIOR LEADER PERSPECTIVE

Achieving Convergence in the Information Environment

Revising the Air Component Structure

Brig Gen George M. Reynolds, USAF



Introduction

The Air Force activated Sixteenth Air Force (AF), a numbered air force focused on information warfare (IW) on 11 October 2019. It was a significant step by the service. The Air Force is not the first military organization to make a meaningful commitment to operating in the information environment. In 2017, the chairman of the Joint Chiefs of Staff added *information* as a joint function to Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*.[1] This revision to joint doctrine signaled the importance of information throughout the Department of Defense (DOD).

All four services are reemphasizing information's importance during planning, execution, and assessments. Information has always been critical to achieving military and national objectives. In fact, nation states and nonstate actors are increasingly turning to IW to achieve their objectives, making now the right time for the US to focus on IW. However, creating an organization responsible for IW with its complex relationships, numerous authorities, and global problems requires

new thinking about how the Air Force organizes operational staffs for employment by joint force commanders.

What is Information Warfare?

The Air Force describes *information warfare* as "the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and armed conflict."[2] IW can deny, degrade, disrupt, deceive, discover, disclose, or destroy the use of information and its functions while also defending against those actions. The objective of IW is to influence or change perceptions, actions, and behaviors in a manner that is consistent with US interests. Typical targets are data, systems, and people. This description of actions, objectives, and targets may sound overly broad such that any military operation or capability could qualify, but contemporary IW is much narrower.

Today's IW integrates the capabilities within the disciplines of weather, public affairs, cyberspace operations, electronic warfare, information operations, and intelligence, reconnaissance, and surveillance (ISR). Each of these disciplines are proven and necessary; however, once under a single operational commander, it can form new, integrated IW options for joint force commanders. Integrating IW disciplines under a force provider can accelerate experimentation, tactics development, specialized planning, professional development, focused intelligence, and operational-level innovation. It is also important to point out that the processes and building blocks IW uses are similar to any military exercise or operation. It requires time-tested actions, including education, training, planning, execution, command and control (C2), and assessments (see fig. 1). These actions must be assigned with clear responsibilities, missions, functions, and tasks.

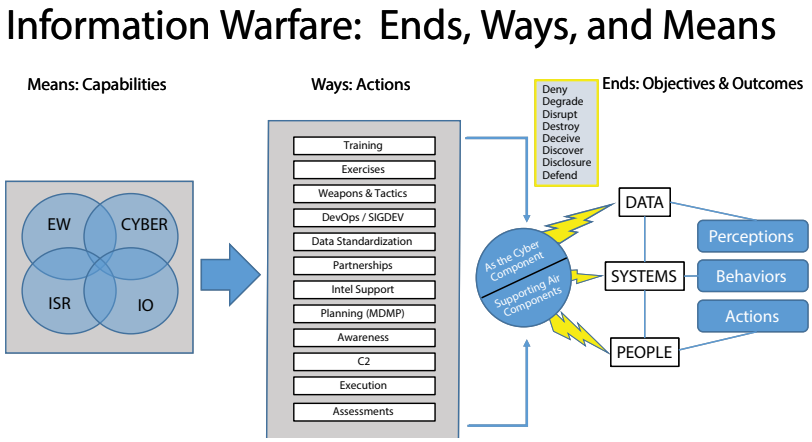


Figure 1. Information warfare ends, ways, and means

Characteristics of Information Warfare

Although IW shares many similar characteristics with other military operations, it possesses some unique challenges and additional complexities. As nations move from competition to conflict in the future, those military organizations that are more agile, adaptive, and able to learn faster can use IW more effectively. A successful organizational design must address four specific operational challenges while also considering process changes to speed up military operations.

IW operations are perishable while coordination takes time. Intelligence preparation, attack access planning, execution, and assessment windows are often perishable and frequently much more so than kinetic operations. Whether a network is no longer accessible, a weapons system changes encryption, or the news cycle moves on to the next event, IW planning and execution requires agility, insights, and the ability to adapt quickly. Conversely, approval processes, tool development, content creation, and other important elements of IW can take significant time and coordination. It is important to note that during counterterror operations, these processes improved, but future complex conflicts will not have the luxury of extended coordination. IW operations will require rapid coordination or even preapproval.

Authorities, forces and capabilities are not centralized. Typically, a single commander or command does not possess all the necessary IW authorities, forces, data access, capabilities, and responsibilities to prosecute an IW mission. Even in those rare cases when a combatant command has most of these assets, the command must coordinate across functional and geographic boundaries to execute a mission.

Achieving integration is challenging. Military operations in and across domains relies on integration. However, achieving IW integration is difficult. Expertise within each IW discipline is specialized, in high demand, and in short supply. IW practitioners may not have experience in integrating their discipline with and across other IW disciplines. There may be limitations with data sharing, clearances, legal concerns with crossing authorities, or simply a lack of opportunities to work with other IW disciplines. Partnerships, exercises, training, mission exposure, and integrated capability development are critical. At its core, IW is an integrated endeavor.

Command and control can be fluid. Supported or supporting relationships can change during a single IW operation and certainly during a campaign. As an example, a single IW operation could:

- Yield insights about adversary capabilities and vulnerabilities for one combatant command

- Create effects for another functional or geographic combatant command
- Provide real-time feedback to an ISR crew supporting yet a third command.

Supported or supporting relationship can change as new information becomes available and mission requirements evolve. The ability of IW forces to support multiple combatant commands and service components fluidly requires partnerships, precoordination, effective delegation of authorities, and clear priorities.

Other military operations can and do share these characteristics, but the design of an effective IW organization must emphasize speed, integration, meaningful partnerships, adaptive processes, and clear lines of responsibility.

Convergence: How Information Warfare is Realized

As outlined in the paper, *16th Air Force and Convergence for the Information War*, "IW convergence is *the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes.*"[3] Convergence occurs during integrated planning and execution in support of combatant commands and their service components, but it also occurs before IW forces are presented. Examples include bringing IW forces together during exercises and training events resulting in new tactics, techniques and procedures (TTP); integrating development operations (DevOps) initiatives creating new, interoperable capabilities; mission rehearsals improving operational integration;[4] implementing data strategies ensuring better access; and experimenting with new and evolving IW concepts leading to improved innovation. Applying the concept of convergence informs how an operational-level organization can fully leverage IW disciplines that generate meaningful outcomes in support of joint force objectives.

Program Guidance Letter Assigned Missions

Sixteenth AF is assigned six specific missions and associated authorities detailed in the Secretary of the Air Force-approved program guidance letter (PGL).[5] These missions include Component-Numbered Air Force (CNAF), Air Force Cyber, Service Cryptologic Component, Defense Intelligence Component Head, Joint Force Headquarters-Cyber Air Force (JFHQ-C (AF)), and responsibility for securing and operating the Air Force Information Network. Each of these missions contain their own responsibilities, authorities, forces, capabilities, access to unique data, and C2 relationships. In most cases, there is natural integration between these missions. Independently, they offer advantages, but together, Sixteenth AF uses each authority distinctly to integrate IW

activities that generate options and outcomes for combatant commands and service components.

Command and Control Model and Organizational Description

Before the activation of Sixteenth AF, Twenty-Fourth AF, and Twenty-Fifth AF had organizational structures unique to their assigned authorities and missions. Twenty-Fourth AF was comprised of a C-NAF staff and operations center and also included the JFHQ-C, Air Force. The JFHQ-C followed a traditional joint task force model with the requisite staff components. It had operational control of assigned cyber mission forces from the Air Force, Army, and Navy, as well as responsibilities for planning, C2, and the execution of cyber operations of these assigned forces. This "joint" headquarters structure was mandated by the DOD and manned by Air Force personnel absent a joint-manning document. Likewise, Twenty-Fifth AF consisted of a numbered air force (NAF) staff and operations center; however, it included the Air Force Cryptologic Office, a staff focused on the service cryptologic component mission. Although each NAF's organizational structure shared similarities, blending their unique authorities, missions, and resources into an IW NAF required a new way to think about Air Force operational organizational design. The traditional component NAF structure was insufficient. Luckily, two component major commands had already begun a similar transformation.

Building upon the Pacific Air Forces (PACAF) and US Air Forces in Europe's (USAFE) new air component models, Sixteenth AF was structured to leverage its distinct authorities, responsibilities, relationships, and multiple staffs while informed by IW's unique operational characteristics and the concept of convergence.[6] This transformation occurred through a series of important steps.

First, Sixteenth AF was activated on 11 October 2019 as a "combined" staff and followed the principle of "doing no harm" to each NAF's missions. The A-staff directorates were led by a single director and supported by cyber and ISR deputies. Additionally, the 625th Operations Center (OC) and 624th OC remained in place, executing their assigned missions.

Second, working with Air Combat Command (ACC), specific operational test and evaluation functions were vertically aligned or divested such as elevating Air Force Inspection Program oversight to ACC, and shifting Joint Worldwide Intelligence Communications System operations to the 688th Cyber Wing.

Third, the 624th OC and 625th OC were deactivated, and the 616th OC was activated on 16 March 2020.

Finally, the ACC commander (COMACC) approved the Sixteenth AF full operating capability (FOC) organizational structure on 19 April 2020 and formally accepted FOC on 13 July 2020.

This COMACC-approved design included an A-staff and a unique IW operations staff consisting of a J-staff, 616th OC, and four cyber operations integrated planning elements (CO-IPE) aligned to United States European Command, United States Strategic Command, United States Transportation Command, and United States Space Command. The four CO-IPEs are aligned to specific combatant commands, supported by the broader Sixteenth AF enterprise. The FOC structure also included IW concepts needed to realize Sixteenth AF's full IW potential. These concepts included:

IW cells. ACC and Sixteenth AF recognized that generating IW outcomes required experts with weather, information operations, electronic warfare, ISR, cyber, and public affairs expertise. As detailed in ACC's *IW Cell Concept Paper*, the "16 AF IW Cell will plan, coordinate, synchronize, and present integrated IW support to air components and CCMDs across the spectrum of military operations and throughout the competition continuum in order to gain and maintain an information advantage."[7] These IW cells will be aligned to unit type codes (UTC), making them available to service component commands to provide surge capacity and IW expertise during exercises and operations. Placing IW cells at the operational level and near the joint force commander not only helps with the creation of IW options but emphasizes the integration of operations in the information environment.[8] As detailed in their paper, *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment*," Gen Mark D. Kelly and Dr. Sandeep S. Mulgund stress the importance of putting OIE at the forefront of component activities.[9] The IW cell provides the added expertise to do this. But the IW cell members also have the right clearances, read-ins, an understanding of combatant command operational plans, relationships with key players, and experience.

Partnership engagement and the political advisor (POLAD). Connecting organizations that operate in the information environment is critical to IW. This connection includes allies, partners, joint organizations, and the interagency. The POLAD plays an important role in understanding changes within international affairs and linking DOD and interagency efforts. Equally important, Sixteenth AF required a Partnerships and Engagement (J54) branch that connects the IW NAF with aligned combatant command and service component operations, activities, and investments and with broader partnership implementation. Having preexisting relationships and partnerships with multiple players is critical to speeding up coordination and cooperation.

Weapons and tactics. As outlined in the PGL, tactics development is critical to IW, but it is about more than the final tactic. The process of creating TTPs strengthens partnership, improves capabilities, integrates IW disciplines, trains and edu-

cates the IW force, and fosters agile innovation. Additionally, resource decisions are informed by these experiences, leading to improvements within DevOps, data sharing, and the convergence of IW disciplines.

IW Operations Staff: Revising the Air Component Structure

Similar to the PACAF and USAFE A3-centric approach, Sixteenth AF focused on the air component structure by creating the IW Operations Staff. It uses the strengths of both an Air Force air operations center (AOC) and Joint Task Force staff. Led by a one-star deputy commander, this IW Operations Staff is responsible for component operations and IW convergence for Sixteenth AF. This staff uses its joint task force staff and AF AOC structures to plan, execute, and assess operations.

To avoid duplicative responsibilities and planning gaps, the IW Operations Staff segmented the joint planning process along a linear time horizon. The AOC is responsible for real-time planning, execution, and assessments, as well as the C2 of assigned forces, including those executing DOD Information Network operations. It also coordinates IW convergence activities with other AOCs during execution. The 616th OC's unique relationships with other AOCs allows for greater awareness, changes to supported and supporting relationships during mission execution, and convergence on emerging problems. The J33 is focused on current operations, the J35 on future operations, and the J5 on long-term planning. The CO-IPEs provide their aligned combatant commands a collocated planning staff. These responsibilities are also detailed in General Kelly and Dr. Mulgund's C2OIE Conceptual Framework. The result is an integrated IW operational staff that not only supports combatant commands and service components but a structure that they can understand—an IW component with a J-staff and an operations center. The transition along the joint planning process from the J-staff to the 616th OC is the strength of the IW operations staff.

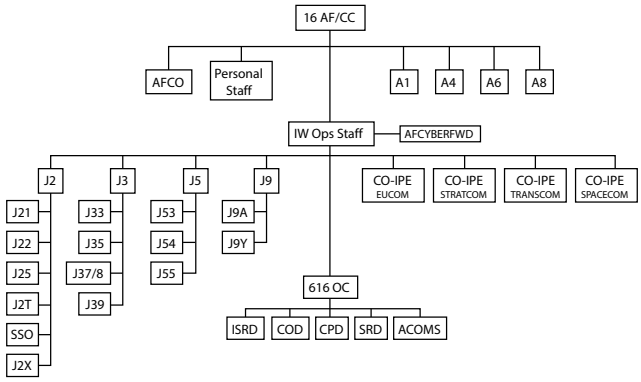


Figure 2. Sixteenth Air Force structure

IW Operations Staff also includes a J2, J5, and J9 under the direction of the IW Operations Staff deputy commander. This alignment not only brings these functions closer to operations and planning but helps eliminate friction points between a staff, AOC, and an empowered A3. The J2 supports the J-staff and cyber mission force's operational-level requirements while staying closely connected to the 616th OC's ISRD. The J5 is responsible for the joint planning group, linking Sixteenth AF to combatant command operational plans and strengthening partnerships through the strategic partnership and engagement division. The J9 conducts assessments, analysis, and lessons learned while working with the assessments team within the 616th OC's Strategy Division. These processes and relationships are critical to IW and require thoughtful coordination between each staff organization. In fact, concept of operations (CONOPS) for planning, intelligence support, assessments, DevOps, a crisis action team, information technology support, and exercises were created to deconflict, then integrate staff missions, functions, and tasks.

These CONOPS are also supported by traditional planning processes and convergence activities. The J3 is responsible for operational planning through an Operations Planning Group, while the J5 leads the Joint Planning Group focused on long-term planning. The J37/8 combines component fires with traditional NAF responsibilities of standardization and evaluation, training, exercises, DevOps, and weapons and tactics. This division's focus is converging IW capabilities through exercises, TTP development, and leading an IW Weapons and Tactics Conference—ultimately, making convergence a reality before forces are presented. The J39 is responsible for integrating information operations, military information support operations, electronic warfare, special technical operations, space, and special programs into IW. Along with the J35, J2, and J54, the J39 provides specialized personnel who support the service component command-aligned IW cell UTCs.

Regardless of how good CONOPS, processes, and relationships are between staff members, the key is an integrated IW operations staff responsible for the prioritization and execution of IW on behalf of the Sixteenth AF commander. The IW operations staff can leverage the assigned authorities, forces, and capabilities to drive staff agility, rapid reprioritization, and IW convergence within an integrated staff.

Way Forward

Creating processes and revising the air component structure are necessary, but organizations need reps and sets to hone their skills, and Sixteenth AF is no exception. Organizational changes will accelerate TTP development, improve training, and create new capabilities. However, planning, executing, and assessing IW

repeatedly is how Sixteenth AF, combatant commands, service components, and joint forces will improve their IW game. More broadly, these same steps are necessary if the DOD is going to compete with adversaries by leveraging operations in the information environment.

As nation-states and nonstate actors increasingly turn to IW, the US's comparative advantage is not guaranteed. Refocusing on IW now provides meaningful options to counter malign influence activities during competition, deescalate crises, and enable success in conflict. Achieving this requires an IW force that can adapt, experiment, take measured risk, and develop clever professionals. This process includes creating an organization that can use IW authorities to integrate activities and generate outcomes for combatant commands and their service components.

The demand for military-based IW options is on the rise. Now is the right time for the Air Force to focus on and integrate IW disciplines to solve military problems, provide commanders additional options for our nation, and change how we organize at the operational level. This focus on complex problems, partnerships, and integrating IW requires a new organizational structure designed for competition and conflict—and one that integrates a staff and operations center as an air component operating at the speed of relevance. ✪

Brig Gen George M. Reynolds, USAF

Brigadier General Reynolds (MS, Gonzaga University; MS, George Washington University; MS, Air Force Institute of Technology) is the vice commander, United States Air Force Warfare Center. His previous assignments include deputy commander, Information Warfare Operations Staff, Sixteenth Air Force (Air Forces Cyber); vice commander, Twenty-Fifth Air Force; and the Air Force Military Fellow, Council on Foreign Relations, New York.

Notes

1. Joint Publication 1, *Doctrine for the Armed Forces of the United States,* 12 July 2017, I-19, https://www.jcs.mil/.

2. *Information Warfare*. According to Draft HAF/A3 Terms of Reference: "The Air Force describes IW as the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and armed conflict. It is distinguished from [operations in the information environment] (OIE) by an increase in the intensity, type, and purpose of activities. Information warfare is an adversary-focused expression of OIE—a subset of circumstances, not a subset of capabilities. Information warfare may be the military purpose of an organization, but the professional competencies and capabilities necessary to conduct it will be equally suited to conducting OIE. Currently, the principal USAF capabilities for IW are CO, EMSO, Information Operations (IO), Intelligence, Surveillance, and Reconnaissance (ISR), and Weather. Critical enablers include, but are not limited to, PA, the Office of Special Investigations (OSI), and the Judge Advocate (JA)."

3. Lt Gen Timothy D. Haugh, Lt Col Nick Hall, and Maj Eugene Fan, USAF, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* 5, no. 2 (Summer 2020), https://cyberdefensereview.army.mil/.

4. DevOps: "Practices which seek to more closely bring together software *dev*elopers and *op*erations staff to work on the same project in a more collaborative manner," https://opensource.com/.

5. Headquarters United States Air Force, Program Guidance Letter 19-05, *Establishment of the Information Warfare (IW) Component Numbered Air Force (C-NAF) under Air Combatant Command*, 6 September 2019, 5.

6. Lt Gen Charles Q. Brown Jr. and Lt Col Rick Fournier, USAF, "No Longer the Outlier: Updating the Air Component Structure," *Air & Space Power Journal* (*ASPJ*) 30, no. 1 (May–June 2016), https://www.airuniversity.af.edu/ASPJ/; and Gen Jeffrey L. Harrigian, Maj Gen Charles S. Corcoran, Col Edward T. Spinelli, and Col John C. McClung, USAF, *Unfinished Business: Refining the Air Component Structure*, *ASPJ* 33, no. 4 (Winter 2019), https://www.airuniversity.af.edu/ASPJ/.

7. Air Combat Command and Sixteenth AF (AFCYBER), "Information Warfare Cell Concept Paper," 28 April 2020.

8. Dr. Sandeep S. Mulgund and Gen Mark D. Kelly, USAF, *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment, ASPJ* 34, no. 3 (Winter 2020), https://www.airuniversity.af.edu/ASPJ/.

9. Kelly and Mulgund, *Command and Control of Operations.*

SENIOR LEADER PERSPECTIVE

Command and Control of Operations in the Information Environment

Leading with Information in Operational Planning, Execution, and Assessment

Sandeep S. Mulgund, PhD
Gen Mark D. Kelly, USAF

Introduction

A broad range of Department of Defense strategic guidance has highlighted the increasing importance of leveraging information to creating enduring strategic outcomes from joint force tactical and operational successes.[1] Advances in information technology are increasing the reach, speed, and effectiveness with which humans acquire, process, and transfer information. State and nonstate adversaries, increasingly unable to challenge the joint force through conventional military power, are using information to gain an advantage over the joint force and impede the achievement of US strategic objectives. The joint force must develop, operationalize, and institutionalize an effective approach for wielding information in concert with traditional physical military power to compete successfully in this environment.

Recognizing its criticality in Joint operations, the 2018 update to Joint Publication 3-0, *Joint Operations* introduced *information* as the seventh joint function.[2] Joint functions are related capabilities grouped together to enable joint force commanders (JFC) to integrate, synchronize, and direct joint operations. The information function encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and support human and automated decision-making. Information can be used as an instrument to affect the behavior of *relevant actors*, which may include any individuals, groups, and populations, or any automated systems whose actions have the potential to substantially help or hinder the success of a particular military activity. As described in JP 3-0,[3] the specific uses of information to affect perceptions, attitudes, and behaviors include:

1. Informing domestic and international audiences through the release of accurate information to put operations in context
2. Influencing relevant actors (not including US audiences) to change or maintain behaviors
3. Attacking and exploiting information, information networks, and information systems

The Joint Concept for Operations in the Information Environment (JCOIE) argues that the joint force must understand how to manipulate and leverage information and the *inherent informational aspects of activities* to send deliberate messages.[4] All Joint force actions, written or spoken words, or displayed or related images have informational aspects that communicate some message or intent, which can be leveraged to support the achievement of Joint force objectives. The JCOIE describes the construct of *informational power* as the ability to leverage information to shape perceptions, attitudes, and other elements that drive desired behavior and the course of events. It establishes the imperative to operationalize and institutionalize the integration of information with traditional military physical power.[5]

Figure 1 illustrates the overall context for operations in the information environment (OIE) and the application of information, as discussed above. Advancing US national interests across the diplomatic, information, military, and economic instruments of national power require affecting relevant actor perceptions and behaviors in a structured manner. This impact happens through operations, activities, and investments (OAI) that may be overt, covert, or clandestine in nature. The intent of those OAIs is to shape the operating environment across

the competition continuum. The results of those OAIs are evaluated through ongoing feedback and assessment mechanisms, which are used to calibrate and refine strategic approaches.

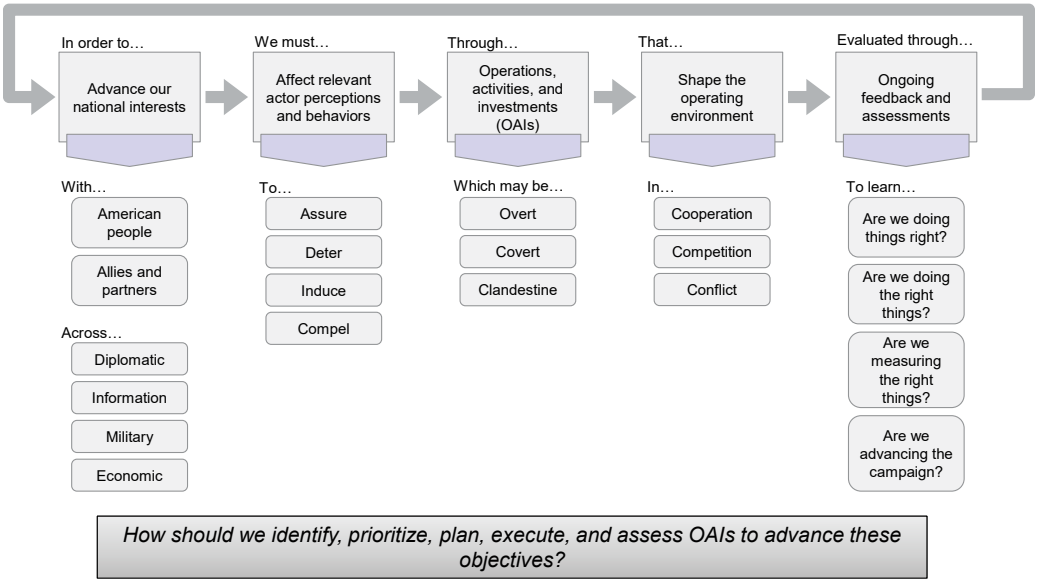


Figure 1. Context for operations in the information environment

The Department of the Air Force has recognized the challenges and opportunities associated with gaining and maintaining information advantage, particularly through the Sixteenth Air Force (AF) standup as an Information Warfare Numbered Air Force. A challenge within the Air Force is that existing constructs for operational-level command and control (C2) (planning, execution, and assessment) do not directly place shaping perceptions and behaviors at the forefront of component activities. This procedure often relegates informational considerations to the end of planners' checklists or treating "information operations" as the realm of specialty teams rather than something central to commander's business. Existing force structures, training programs, and associated command relationships are not designed to facilitate the effective integration of informational power considerations into operational-level C2, which is oriented to the air tasking cycle for combat operations. This approach described in this article seeks to address these challenges by defining approaches to placing information at the forefront of air and space component operational planning, execution, and assessment processes and approaches. It complements the approach described by General Reynolds to develop an organizational structure for information warfare at Sixteenth AF.[6]

Conceptual framework

Figure 2 below presents the overall C2OIE conceptual framework, the purpose of which is to establish how to incorporate the joint function of information into operational-level planning, execution, and assessment processes.[7]

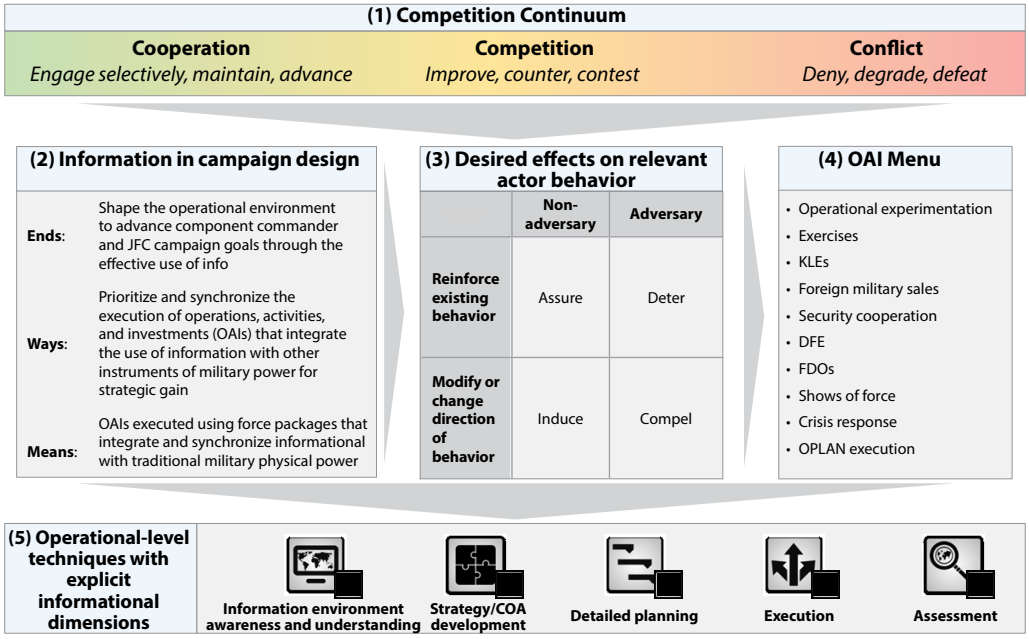


Figure 2. C2OIE conceptual framework

Each of the elements in figure 2 is described further below.

(1) Joint force activities occur across the continuum of cooperation, competition, and armed conflict,[8] each with specific policy objectives. The effective application of informational power is of central importance for creating an advantage and attaining enduring strategic outcomes in each part of the continuum.

(2) Deliberate, long-term campaigns are a key means to shape relevant actor perceptions and behaviors across the continuum, by capitalizing on the cumulative and reinforcing effects of multiple, coordinated OAIs. Air and space component level efforts support the achievement of JFC strategic outcomes through the design and execution of nested campaigns and OAIs that integrate the employment of informational power and physical power in coordination with the rest of the joint force.

(3) The goals for individual activities that comprise the overall campaign are expressed in terms of the desired effects on relevant actor behavior. For simplicity, relevant actors are either adversaries or nonadversaries, and the desired effects

on their behavior may be to reinforce existing behaviors or bring about a change in behavior.

(4) Forces and capabilities that wield informational power and physical power are integrated into component OAIs selected and designed to create the desired effects on relevant actor behavior.

(5) A set of practical techniques provide a structure for incorporating the information joint function into overall OAI planning, execution, and assessment.

OIE across the Competition Continuum

Joint Doctrine Note 1-19 introduces the competition continuum as a way of describing a comprehensive and flexible spectrum of strategic interactions, engagements, and relations between the United States and other actors.[9] Rather than the binary classifications of peace and war, the competition continuum describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict. These descriptors refer to the relationship between the US and another strategic actor (state or nonstate) in relation to a set of specific policy objectives. The competition continuum describes the environment in which the US government applies the instruments of national power. Key points on the continuum are:

Cooperation: mutually beneficial relationships between strategic actors with similar or compatible interests

Competition: relationships between actors with incompatible interests—none of whom seek to escalate to armed conflict

Armed conflict: a situation in which the of violence is the primary means by which an actor seeks to satisfy its interests

Crises can occur anywhere along the continuum, and the term *confrontation* can be used to describe conditions between competition and conflict. The United States may be in different parts of the continuum in its interaction with a single actor in relation to different interests. OIE play a key role across the entirety of the continuum to support creating, maintaining, and exploiting overall joint force advantage, as illustrated below in figure 3.

The figure shows representative OIE activities across the competition continuum that can be used to create and leverage *information advantage*—conditions in the IE favorable to achieving the commander's overall objectives—through campaign activities that are integrated and coordinated in purpose.

	Cooperation	Competition	Conflict
Policy objectives	*Engage selectively, maintain, advance*	*Improve, counter, contest*	*Deny, degrade, defeat*
OI support to policy objectives	• Expand competitive space with allies and partners through development and demonstration of enhanced information sharing, cooperative agreements, and activities • Conduct military engagement in support of humanitarian response • Synchronize messaging with allies and partners to demonstrate strength of cooperative security agreements • Attract new security partners by communicating presence and commitment	• Diminish adversary's competitive space by countering/frustrating their narrative, and influencing them to divert their resources towards unproductive ends • Expose and counter malign influence • Counter disinformation and propaganda • Reinforce international norms and the collective benefits of adherence • Mislead adversary decision-makers on Joint force dispositions, capabilities, and vulnerabilities to impose costs by diverting their cognitive or physical resources towards unproductive ends • Conduct selective demonstrations of unique Joint force capabilities	• Neutralize enemy's will and capabilities to fight • Provide offramps for conflict resolution • Provide transparent response to accidents or inadvertent events • Deceive enemy decision-makers on Jount force dispositions, capabilities, intentions, and actions to create operational surprise • Deny enemy freedon of action in cyberspace and the electromagnetic spectrum (EMS) while ensuring it for the Joint Force
Examples	 **Humanitarian assistance/ disaster response** *Movement/maneuver, protection, sustainment, and information*	 **Operation RAPID FORGE Dynamic Force Employment** *Information amplifying C2, movement/ maneuver, and sustainment*	 **Afghanistan MOAB** *Fires in support of information*

Figure 3. OIE across the competition continuum

Campaign Design

Campaign activities focus on a command's day-to-day activities to create such effects through the conduct of operations, military engagement, security cooperation, deterrence, and other shaping or preventive activities.[10] They are a *series* of related OAIs aimed at accomplishing strategic and operational objectives within a given time and space. Campaigns comprehensively and coherently link all steady-state activities and contingency operations within a unifying framework. Air and space component campaigns nest underneath combatant command campaign plans and global campaign plans.[11] The table proposes component campaign ends, ways, and means from an informational perspective.

Table. Campaign-level informational ends, ways, and means

Ends	• Shape the operational environment to advance component commander and JFC campaign goals through the effective use of information to affect relevant actor perceptions and behaviors • Increased understanding and trust with domestic and international audiences in the purpose of and approach to component activities • Erosion of adversary confidence in their capabilities, strategies, and relationships • Diminished enemy ability to sense, understand, decide, and act effectively
Ways	• Prioritize and synchronize the execution of OAIs that integrate the use of information with other instruments of military power for strategic gain • Establish overall component narrative and key themes, and allocate resources in accordance with and in support of them • Align component-level OAIs with a common and consistent narrative • Synchronize efforts across components and AORs with mission partners • Continually reinforce the component narrative through sustained presence and engagement in the IE, proactively and in response to emergent events across the competition continuum • Assess effects in support of JFC campaign objectives and refine campaign approach
Means	• OAIs executed using responsive force packages that integrate and synchronize informational power with traditional military physical power

Effects on Relevant Actor Behavior

The purpose of campaign activities is to shape the attitudes, perceptions, and behaviors of applicable relevant actors in a manner beneficial to U.S. interests. Figure 2 above presents a 2x2 model for describing desired effects on relevant actor behaviors. Drawing from Barry Blechman and Stephen S. Kaplan,[12] relevant actors are categorized as either *adversaries* or *nonadversaries*, for simplicity. Nonadversaries include a broad range of actors, who may be allies, partners, or neutral third parties. Using the language of coercive diplomacy, the purpose of using military forces and capabilities may be to *reinforce* existing behavior or to *modify or change* the direction of behavior. These axes combine to describe four possible modes for the use of military forces and capabilities to affect relevant actor behavior in support of campaign-level ends:

1. *Assuring* nonadversaries so that they will continue or abstain from a behavior relative to US interests. The emphasis here is on easing the concerns of allies and partners so that they will continue behaviors beneficial (or abstain from behaviors detrimental) to US interests.
2. *Deterring* adversaries from behavior that is detrimental to US interests. The goal of deterrence is to prevent an action through a credible threat of unacceptable counteraction and/or belief that the cost of an action will outweigh its perceived benefits, combined with ensuring the availability of off-ramps to allow the adversary to de-escalate the situation.
3. *Inducing* nonadversaries to initiate beneficial actions or halt actions contrary to US interests.

4. *Compelling* adversaries to act in a manner or stop acting in a manner contrary to US interests, through the credible threat or actual use of force.

Application of Information Power in Air and Space Component OAIs

Campaigns are executed through a series of OAIs, spanning day-to-day operations through crisis response. From an OIE perspective, critical to the selection and design of each OAI is its ability to shape the IE to advance component or combatant command objectives as discussed above, using capabilities and approaches appropriate to the circumstance. Categories of OAIs include:

- **Operational tests and experimentation**. Demonstration and evaluation of new military capabilities or approaches, potentially with the ability to affect the status quo between actors
- **Exercises**. Military maneuvers or simulated wartime operations involving planning, preparation, and execution, carried out for the purpose of building, improving, maintaining, and evaluating proficiency at key mission areas
- **Force posture**. Forces rotationally deployed as well as permanently stationed abroad, together with the facilities and supporting infrastructure that make up the US military footprint and the agreements that enable this presence
- **Key leader engagements**. Engagements by a commander with principal local and regional leaders in the operational environment
- **Foreign military sales**. Transferring defense articles, services, and training to US international partners and international organizations.
- **Security cooperation**. Interactions with foreign security establishments to build security relationships that promote specific US security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to allied and partner nations
- **Dynamic force employment**. Strategically predictable but operationally unpredictable use of the force executed to exploit emergent or anticipated strategic opportunities
- **Flexible deterrent options**. A planning construct that provides a wide range of interrelated responses that begin with deterrent-oriented actions carefully tailored to produce a desired effect[13]

- **Shows of force**. The demonstration of resolve involving increased visibility of deployed forces in an attempt to defuse a situation that, if allowed to continue, may be detrimental to US interests or objectives[14]
- **Crisis response**. The execution of a response to an incident or situation involving a threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national objectives[15]
- **Operations plan execution**. The execution of a complete and detailed plan for a contingency, containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment list

Each of these categories of OAIs have inherent informational aspects that can be shaped and leveraged to assure, induce, deter, or compel relevant actors of interest. Operations in the information environment can directly enable, support, and reinforce them as described earlier in the table. Combining informational power with physical power in individual OAIs creates reinforcing effects by maximizing the value of each through appropriate relative timing, tempo, scope, and purpose. In so doing, it maximizes their combined ability to create advantage for the Joint force. Individual OAIs are part of an overall campaign of activities, per the table above. Figure 4 illustrates the potential linkages between physical power and informational power actions from a temporal perspective—before, during, and after the employment of military physical power. Before a physical power action, informational power may be used in an enabling capacity:

- To create physical conditions for success (e.g., electronic warfare activities and offensive cyberspace operations)
- To impose costs by drawing or diverting an actor's attention from the true purpose and nature of joint force actions (e.g., military deception)
- To shape relevant actor expectations through overt/covert messaging to support assurance and deterrence, while mitigating an adversary's ability to mislead or misinform audiences

During the employment of physical force, informational power can act in a supporting and enhancing way. Alternatively, the physical power action may be simply to demonstrate the will behind a comprehensive set of OIE. Finally, following the employment of physical force, informational power can be used to reinforce impressions and interpretations of what has occurred and condition relevant actor expectations for what might happen next. Such a coordinated approach enables joint force commanders to take the initiative in the information environment, rather than being reactive to adversary actions.

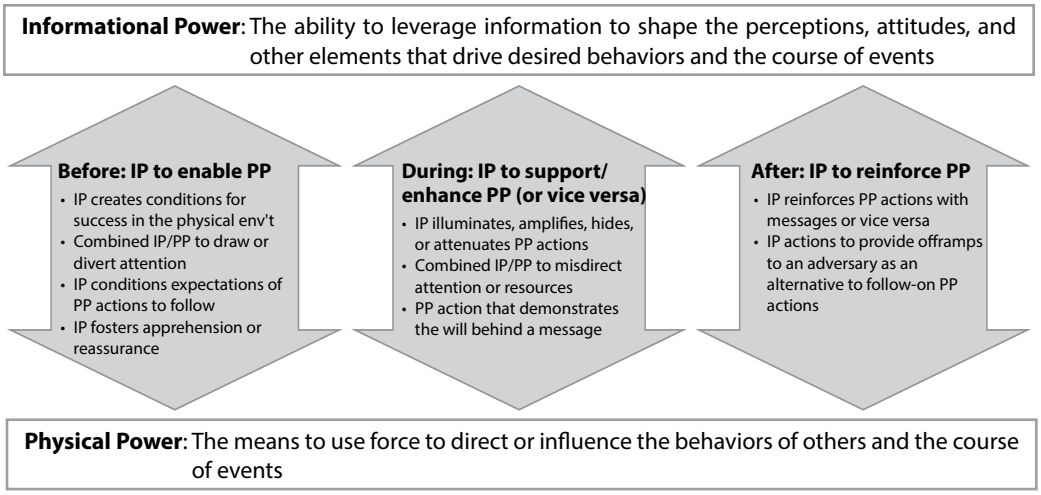


Figure 4. Integration of informational power and physical power

Such combined actions require both *integration* and *synchronization*—integration in planning requires choosing an effective combination of informational and physical effects to drive the desired relevant actor behavior, predicated upon an understanding of the operational environment. Synchronization in execution converges those effects with the right timing, tempo, scope, and intensity. It should be noted that different OAIs may call for different degrees and weights of informational power and physical power. For example, military engagement or security cooperation activities focused purely on exposing and countering malign influence or disinformation may have little to no physical power element and rely principally on OIE to affect relevant actor perceptions and behaviors.

Operational-Level Techniques

The final portion of the model is a set of information-focused approaches to OAI planning, execution, and assessment to be used as part of overall joint planning process efforts,[16] summarized as follows:

• **Information environment awareness and understanding** focuses on developing and maintaining an integrated understanding of the information aspects of the operational environment spanning geographic, functional, domain, classification, and organizational boundaries. Understanding the information environment is an element of understanding the operational environment as a whole.

• **Strategy and course-of-action development** focuses on the establishment of the operational approach to shape relevant actor behavior and perceptions

through integration of information with other instruments of military power, leveraging the inherent informational aspects of activities.

• **Detailed planning** focuses on building integrated, executable force packages to create desired effects using informational and physical power wielded through assigned, attached, and supporting forces and capabilities.

• **Execution** synchronizes the creation of integrated effects using informational and physical power and adapting the approach as commander's guidance and evolving circumstances require.

• **Assessment** centers on evaluating effects created or occurring against relevant actor perceptions, behavior, and capabilities and on identifying new opportunities to advance overall JFC objectives.

Well-established component-level tactics, techniques, and procedures (TTP) exist for each of these activities. The emphasis in this new Department of the Air Force framework is on bringing the information joint function to the forefront and placing the focus in each set of activities on shaping relevant actor perceptions, attitudes, and behaviors. The depth to which each of these steps must be pursued will be a function of the complexity of the OAI, whether it is an extension of an ongoing activity, the availability of "off-the-shelf" plans, and other related considerations.

Summary

This article has presented a preliminary approach for bringing information to the forefront of air and space component operational-level planning, execution, and assessment. This approach entails designing component operations directly around shaping the perceptions and behaviors of relevant actors and target audiences of interest, rather than the incorporation of information operations as an afterthought to kinetically focused planning methods. Concepts in this article will continue to evolve through their application in ongoing and future air component campaigns and OAIs to enable their validation and refinement. Specific areas for refinement and evolution include:

- Practical measures of effectiveness (MOE) and MOE indicators
- Elements of effective narratives
- Intelligence collection and analysis requirements
- OIE assessment methodologies
- Command relationships and authorities for responsive OIE
- Materiel solution enablers
- War-gaming approaches
- Integration with a wide range of mission partners

Insights from these efforts will enable evolving the preliminary planning, execution, and assessment techniques in this document into comprehensive and authoritative air and space component TTPs that drive air and space force operational practice and training curricula. ✪

Sandeep S. Mulgund, PhD

Dr. Mulgund (BASC, University of Toronto; PhD, Princeton University) is a highly qualified expert senior advisor to the Deputy Chief of Staff for Operations (AF/A3). He is leading the A3's efforts to evolve air component approaches to operational-level planning, execution, and assessment to more effectively incorporate operations in the information environment as part of the Air Force's overall approaches for joint all-domain operations.

Gen Mark D. Kelly, USAF

General Kelly (BA, Southwest Texas State University; MMAS, Air Command and Staff College; MS, National War College) is the commander, Air Combat Command, Joint Base Langley-Eustis, Virginia. As the commander, he is responsible for organizing, training, equipping, and maintaining combat-ready air, space, cyber, and intelligence forces for rapid deployment and employment while ensuring strategic air defense forces are ready to meet the challenges of peacetime air sovereignty and wartime defense.

Notes

1. Joint Concept for Operating in the Information Environment (JCOIE), https://www.jcs.mil/, July 2018; Department of Defense (DOD), *Department of Defense Strategy for Operations in the Information Environment*, https://dod.defense.gov/, June 2016; DOD, *Summary of the 2018 National Defense Strategy of the United States of America*, 2018, https://dod.defense.gov/; and DOD, *Department of Defense Strategy for Operations in the Information Environment*, https://dod.defense.gov/, June 2016.
2. Joint Publication (JP) 3-0, *Joint Operations*, https://www.jcs.mil/, October 2018.
3. JP 3-0, *Joint Operations*.
4. DOD, *Department of Defense Strategy for Operations in the Information Environment*.
5. JCOIE, July 2018.
6. Brig Gen George M. Reynolds, USAF, "Achieving Convergence in the Information Environment," *Air & Space Power Journal* (*ASPJ*) 34, no. 3, https://www.airuniversity.af.edu/ASPJ/.
7. JP 3-0, *Joint Operations*.
8. Joint Chiefs of Staff (JCS), Joint Doctrine Note 1-19, "Competition Continuum," June 2019, https://www.jcs.mil/.
9. JCS, Joint Doctrine Note 1-19.
10. JP 5-0, *Joint Planning*, June 2017, https://www.jcs.mil/.
11. Chairman of the Joint Chiefs of Staff Instruction 3100.01D, *Joint Strategic Planning System*, https://www.jcs.mil/, July 2018.
12. Barry Blechman and Stephen S. Kaplan, F*orce Without War: U.S. Armed Forces as a Political Instrument* (Washington, DC: Brookings Institution, 1978).
13. JP 5-0, *Joint Planning*.
14. Blechman and Kaplan, F*orce Without War: U.S. Armed Forces as a Political Instrument* (Washington, DC: Brookings Institution, 1978).
15. *Department of Defense Dictionary of Military and Associated Terms*, https://www.jcs.mil/.
16. JP 5-0, *Joint Planning*.

FEATURE

Restructuring Information Warfare in the United States

Shaping the Narrative of the Future

Capt Anthony J. Eastin, USAF
1st Lt Patrick G. Franck, USAF*

Introduction

On 31 December 2019, the People's Republic of China (PRC) verified to the World Health Organization (WHO) that pneumonia of an unknown cause was reported in Wuhan, China. This virus would later be known as COVID-19.[1] On 10 January 2020, the PRC reported its first COVID-19 casualty. Two days later, the virus made its first appearance outside of mainland China and on 21 January

*This work would not have been made possible without the help and support of various individuals in the US Air Force and colleagues across the Department of Defense (DOD), Department of State, and academia. We would especially like to thank Lt Col Matthew Linford, PhD, who helped shape and guide this article; he was an instrumental part in the work you see here today. We would also like to thank Dr. Robert Ehlers, Colonel, USAF, Ret., and Lt Col Brian Johnson for their feedback and expertise in understanding our current DOD information operations construct. We would also like to thank Joint Information Operations Warfare Center members for their insightful feedback on their organization and authority limitations. Lastly, we would like to individually thank Lt Col Armin Blueggel, Lt Col Nikita Belikov, Maj Julie Janson, Maj Erik Armbrust, Maj Madeline Goff, David Bryan, Stephanie Hebert, and Haley Wilson. Their insightful feedback was invaluable in earlier versions of this article.

2020, the US announced its first COVID-19 case.[2] In an attempt to downplay the dangers of the virus, deflect blame, and ultimately protect its interests, the PRC waged a complex, multifaceted information warfare (IW) campaign.[3] The PRC intentionally suppressed information to the public from its health experts, carefully crafted narratives across all media platforms that: 1) favorably highlighted its response to the virus, 2) blamed the US in the spread of the virus, and 3) compared the virus to the common flu.

Although not as easily observed and understood as physical warfare, the effects of this IW campaign are equally devastating. The confusion created by this campaign caused the world to delay recognizing the seriousness of the pandemic, created doubts and uncertainty regarding the best way to handle the virus, and enabled its rapid spread. This confusion contributed to the US losing more lives to the virus than the Vietnam War and all subsequent armed conflicts in which the country has been involved.[4]

The United States government (USG) has long recognized the need to increase its ability to operate in the information environment (IE).[5] Although some progress has been made, the US remains woefully unprepared to combat complex IW campaigns such as the one waged by the PRC. This inability has harmed US interests and increased the economic cost and total lives lost. The US must quickly close the strategic gap in its ability to operate in the IE and counter adversary IW campaigns by developing a whole-of-government organization similar in scope to the defunct US Information Agency (USIA)—directly linked and colocated with fully resourced and empowered Department of Defense and Department of State counterparts.

PRC's Information Warfare Campaign

In line with the PRC's unrestricted warfare doctrine, some analysts have argued that once confirmed that their economy would be negatively affected by COVID-19, its "strategic competitiveness moving forward was critically dependent that the economies of its strategic rivals should also be forced into decline." In an analysis, the PRC's IW campaign appeared to be geared toward protecting PRC investments and increasing the cost of COVID-19 for its strategic rivals.[6]

Initially, the PRC focused on two main efforts: suppressing information and creating misinformation. The PRC suppressed potentially damaging information that it perceived as endangering its worldwide investments. Simultaneously, through the use of social media and strategic messaging, they rapidly disseminated false information in an attempt to highlight its ability to deal with the pandemic, deflect blame regarding the cause of the pandemic, and create an overall sense of confusion about the virus to protect itself and its investments across the world.

Suppressing Information—How the Virus Spreads

Evidence shows that the virus was spreading via human-to-human transmission as early as 1 December 2019.[7] On 27 December 2019, Dr. Zhang Jixian reported a family cluster of cases to her superiors, indicating the virus was spreading via person-to-person.[8] On 30 December 2019, Dr. Ai Fen reported an unknown respiratory virus to her superiors.[9] Instead of acting on the information, her superiors reprimanded her. She recounted the admonishment in an essay titled, "The One Who Supplied the Whistle," published in *China's People* (*Renwu*) magazine. Following publication, the article was deleted from Chinese social media sites, removed from *Renwu* magazine, and Dr. Ai was reported missing.[10] Despite the PRC's attempt to suppress the article, Chinese citizens found creative ways to avoid the PRC's censorship. Writing the article backward, inserting intentional typos and emojis, and sharing the article in fictional languages such as Klingon, allowed the article to spread through various platforms.[11]

Similar to Dr. Ai Fen, Dr. Li Wenliang warned his colleagues and publicly shared his findings about a possible outbreak of a highly infectious respiratory disease.[12] On 2 January 2020, Wuhan police, governed by the PRC's Ministry of Public Security, summoned Dr. Li and his colleagues and threatened to detain them for "making false comments on the Internet."[13]

With the success of the PRC's suppression efforts, Wuhan, with more than 11 million people and 800,000 tourists per year, continued to operate as usual through a Chinese Communist Party conference held on January 12–15 with authorities claiming zero new cases in this period. The PRC would not confirm human-to-human transmission of the virus until 22 January 2020.[14]

With little contrary evidence to show otherwise, due in part to the PRC suppressing information, the WHO announced on 14 January 2020 that "preliminary investigations conducted by the PRC found no clear evidence of human-to-human transmission of the novel coronavirus (COVID-19) identified in Wuhan, China."[15] Had the WHO known that in early December, multiple Chinese doctors had reported patients with COVID-19 like symptoms—with no exposure to the South China seafood market—they may have issued alternative guidance.[16]

Suppressing Information-Number of Cases in China

Although the PRC has since conceded the virus has a high likelihood of spreading via human-to-human transmission, it continued to suppress the number of COVID-19 deaths across China. As of 8 October 2020, officials in China reported 91,252 citizens had tested positive for COVID-19, and 4,634 had died from the virus; meanwhile, New York City reported 473,000 people had tested

positive, with more than 32,850 dying from the virus.[17] Given the population size and density of China (1.4 billion) and New York City (8.4 million), it seemed improbable that the entire country of China would have only one-seventh the deaths of New York City.

Despite the PRC's attempt to control that narrative, the international community began to openly criticize China and doubt the validity of the data released. Reports of trucks delivering thousands of urns per day in Wuhan, crematoriums unable to keep up with the demand necessary to discard the bodies, and Wuhan citizens speaking up against the PRC's claim of a low mortality rate contributed evidence to counter their claims and helped expose the PRC's IW campaign.[18]

With increased pressure from the international community and domestic activists on 17 April 2020, the PRC revised its total number of COVID-19 cases by increasing its death toll exactly 50 percent and adding 1,290 fatalities.[19]

Creating Disinformation

As analysis demonstrates above, the PRC began their disinformation campaign by minimizing the virus's risk of spreading via human-to-human transmission. They would later evolve their disinformation campaign by minimizing the virus's effects and later blaming the US for the pandemic.

The "It's Just a Flu" Narrative

The "it's just a flu" narrative can be traced back to early January when social media posts surfaced to downplay the seriousness of this new threat by relating it to seasonal influenza and emphasizing that the traditional flu is deadlier than COVID-19.[20] First emerging via *Twitter* posts, the narrative was subsequently picked up and propagated widely via bot-like behavior. Although these accounts cannot be traced to any specific adversaries, they follow similar tactics employed by past PRC IW campaigns.[21] Chinese state media outlets ran pieces discussing the current US flu season during this time, portraying it as a parallel and comparable epidemic. Foreign Ministry officials exploited these stories by citing US seasonal flu numbers to counter criticism over the PRC's handling of the situation. They would later downplay the coronavirus as the flu by propagating misleading statistics that encouraged people to make false comparisons between COVID-19 and the H1N1 outbreak; to this day, this narrative continues to be supported and propagated across the US.[22]

US Biological Weapon Narrative

On 23 February 2020, a PRC official state newspaper reprinted an article associating the US seasonal influenza deaths with the novel coronavirus, causing speculation that COVID-19 originated in the US. Additionally, the PRC amplified these articles and social media posts alleging the virus was a result of the USG.[23]

On 27 February 2020, a Chinese doctor, Zhong Nanshan, stated that the virus "may not have originated in China." Soon after, numerous Chinese politicians began what appeared to be a coordinated information campaign to spread this narrative.[24] On 8 March 2020, the Chinese ambassador to South Africa tweeted that, "Although the epidemic first broke out in China, it did not necessarily mean that the virus originated from China, let alone 'made in China'"[25] South Africa is a key member of China's Belt and Road initiative; it was in China's best interest to shift blame to the US to ensure that its investments worldwide and in South Africa were protected. On 8 April 2020, South Africa's President Cyril Ramaphosa expressed "gratitude to China for its long-term support to South Africa and African countries," a significant indicator of a successful campaign.[26]

Along with traditional media, social media sites like *Facebook*, *Twitter*, and *YouTube* saw growth in posts asserting that the virus may have been a funded US biological weapon. *Google Trends* analysis also indicates that these narratives were highly prevalent with individuals worldwide searching whether the virus was a result of US malfeasance—an indication of the success of this disinformation campaign.[27]

The PRC spread and amplified multiple disinformation narratives across multiple platforms, continuing to cause widespread confusion in the IE. The successful suppression campaign conducted by the PRC deprived the WHO and other world leaders of vital evidence. The WHO would later claim that the spread of false information resulted in an "infodemic" with people across the globe unable to find reliable information surrounding COVID-19.[28] Despite numerous efforts from information companies, US officials, and health experts, conspiracy theories and ineffective preventative measures continue to flood the IE and discredit the USG's response to the pandemic.[29]

Structural Challenges to Countering Global IW Campaigns

The inability to quickly identify the PRC's IW campaign and mount an effective response highlights the US's inability to combat complex, multifaceted IW campaigns. This inability centers on the fact that US IW capabilities are spread across numerous entities, and there are no sufficient structures in place from which the US can conduct a whole-of-government response. Other USG instruments of national power have a lead in coordinating its use (State Department for Diplo-

matic, the Department of Defense for Military, and—for simplicity of argument—the Department of Treasury for Economic). However, the US has no lead agency to organize, coordinate, synchronize, and, most importantly, task other government entities to employ information as an instrument of national power.

While there are different organizations across multiple USG agencies capable of employing information as an instrument of national power, the lack of a centralized and coordinated IW response results in a dispersed capability with individual organizations lacking the resources or authorities to effectively engage and protect US interests. When organizations do engage, there is a lack of a synchronized and cohesive narrative. These limitations leave the US unable to provide a real-time, whole-of-government approach to address adversary IW campaigns or actively shape the IE during times of heightened competition.[30] To highlight this point, we explore several of the main USG agencies that operate in the IE.

US Agency for Global Media

Countering IW was not a new need for the US. The Cold War was rife with Soviet attempts to control the IE.[31] To counter that challenge, the USIA was created in 1953.[32] At the height of the Cold War, the USIA had an annual operational budget of $2 billion and employed a professional staff of over 10,000 spread across 150 countries; it also had the authority to protect US interests in the IE. Following the Cold War, the USIA was disbanded, and its broadcasting functions were consolidated under an independent entity known as the US Agency for Global Media (USAGM).[33]

With a drastic cut in resources and mission, the USAGM now serves as the governing body for all nonmilitary US broadcasting, providing programming in 56 languages. The USAGM mission is to inform, engage, and connect people worldwide in support of freedom and democracy. However, unlike its predecessor, the USAGM lacks the authority, and is not chartered, funded or equipped to conduct broad operations in the IE to counter adversarial propaganda and misinformation. Although USAGM is one of the most globally aligned US organizations available to counter IW campaigns, it is under-resourced and does not possess the requisite authorities to do so.[34]

Department of Defense

The DOD has IW capabilities at various levels within its force. Most reside inside the force structure of geographic and functional combatant commands (CCMD) and are tasked through unified combatant command (COCOM) authority, the nontransferable authority to command, and task assigned forces to

accomplish missions.[35] Due to the sensitive nature and strategic implication of some of these capabilities, authorities to utilize IW capabilities are often retained by the Secretary of Defense (SECDEF) or president of the United States (POTUS). This structure creates a myriad of capabilities and authorities residing in geographic CCMDs such as the United States Indo-Pacific Command, and in functional combatant commands such as United States Cyber Command (USCYBERCOM). Although the DOD utilizes the concept of supported and supporting commands to clarify the relationship between commands engaging in the same conflict, there are few distinct geographic or functional lines in IW, making the designation of supported and supporting commands problematic.[36] The Joint Information Operations Warfare Center (JIOWC) is the DOD's only strategic-level IW entity not aligned to a command. Reporting directly to the chairman of the Joint Chiefs of Staff, it is uniquely situated to enable the DOD's information power across the globe. However, under the CJCS, it does not have COCOM authority and has no tasking authority over those who do.

Further complicating the DOD employment of IW capabilities is the fact that "many of our defense establishment processes presuppose clearly defined states of peace and war."[37] To limit US war-fighting advantages, adversaries utilize IW to compete in a manner that seeks to avoid triggering open conflict.[38] When no area of active hostilities has been designated, DOD IW capabilities to compete with adversaries below the armed conflict level are often bogged down with a complex approval process. By the time approvals are granted, the IE has evolved, and the opportunity to shape and influence the IE has often been missed.

Department of State

The Department of State (DOS) has multiple capabilities to conduct operations in the IE—most are nested under the chief of mission (COM) in a given country. The authority to execute operations in the IE (OIE) occurs under the COM.[39] With COM authorities designated by country, the authority to utilize DOS IW capabilities when the threat expands geopolitical boundaries is complex and time-consuming.

The DOS also has a global IW organization, the Global Engagement Center (GEC). The GEC is tasked to "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining U.S. security interests."[40]

The GEC's global nature makes it uniquely situated among DOS entities to identify IW campaigns similar to one the PRC is currently waging. Although the GEC enjoys a broad charter in the OIE of a given country, tension often

comes between COM country-specific authorities and GEC's global charter. What is best for the global or regional operation may counter a COM's given mission and vision. As currently organized, the GEC has not been given broad authorities to conduct OIE but has instead been relegated to "as needed, *support* the development and dissemination of fact-based narratives and analysis to counter propaganda and disinformation directed at the United States."[41] Also, despite having an essential global tasking, the GEC has historically been under-resourced and under-utilized.

Recommendation

The USG structure analysis related to IW concluded that the USAGM, DOD, and DOS do not, individually, have the resources or authorities to adequately compete in the IE. These organizations and departments independently provide the US capabilities; however, structural, geographical, functional, or legal limitations leave the USG response disjointed, unsynchronized, and ineffective against complex, multifaceted global IW campaigns.

For the US to compete in the IE, it requires a whole-of-government approach to rapidly mobilize resources and capabilities to reduce the spread of disinformation and counter adversary tactics that endanger US citizens, such as the one which was conducted by the PRC. Our recommendation is to create an independent, whole-of-government organization reporting directly to the National Security Council that will be empowered and resourced to lead, synchronize, and task IW capabilities to defend and protect US interests. This organization should be similar in scope to the defunct USIA, which existed from 1953–99, to counter Soviet messaging. An effort of this magnitude or greater is required for the US to compete successfully with China, Russia, Iran, and other potential competitors in the IE.

The inability to counter a complex IW campaign will not be the fault of any of these organizations or departments. As briefly outlined in the IE analysis, the US inability to respond to IW has been viewed as an organizational structure problem. The lack of a single, fully resourced government function has left the US with fragmented, under-resourced, and under-authorized entities doing the best they can against well organized and equipped adversaries. Unfortunately, numerous IW campaigns against the US and its citizens, such as the one highlighted above, confirms that the US approach results in delayed, disorganized responses and missed opportunities to counter complex IW campaigns and favorably shape the IE.

A whole-of-government organization, built to compete in today's IE, should be empowered to lead, synchronize, and coordinate USG diverse and previously separated IW capabilities across the conflict continuum to protect the US, its in-

terests, and allies. The broadcasting capabilities of the USAGM should be fully absorbed into the new organization, and the USAGM dissolved. The GEC could serve as a core of this new organization and represent the DOS in this whole-of-government approach. The JIOWC, or a similar DOD organization, should be colocated with this new organization to enhance effective coordination, synchronization and to ensure DOD support is available when needed.

Furthermore, this new organization should be granted additional chief of information warfare authorities. These authorities should include the ability to task disparate IW capabilities resident in other government entities to support the US in defense of broad IW campaigns that do not neatly fit within the scope of COM or COCOM authority.

We also recommend the DOD internally restructure to optimize for IW. Much of this restructuring is already underway with joint concepts such as the Joint Concept for Integrated Campaigning and the Joint Concept for Operations in the Information Environment guiding the way. The component efforts must be supplemented by a larger, more strategic reorganization that allows for a whole of DOD approach to be nested within the whole-of-government approach.

One of the challenges of the DOD's current approach of placing war-fighting authorities under COCOM authorities is limiting authority by geographic location or war-fighting function. IW is neither geographically nor functionally limited. Under the current structure, the geographic CCMDs are perhaps best aligned to compete in the IE's physical dimensions, USCYBERCOM to operate in the information dimension, and United States Special Operations Command has the expertise and capabilities to operate in the cognitive dimension. These dimensions' interrelated nature will always create confusion where one CCMD's COCOM authority begins, and another's authority ends when competing and waging conflict in the IE. Although the concepts of supported and supporting help clarify roles and responsibilities in war fighting, giving primacy to one CCMD in the IW fight would unintentionally place geographic or functional limitations on the US ability to respond.[42]

One approach to solving this dilemma would be to pull the JIOWC up from its current location under the CJCS or stand-up a new, similar organization and place it under the direct authority of the SECDEF. With the IE as its sole concentration, this entity laser-focus on understanding the global IE, recognizing IW campaigns and SECDEF tasking authorities tasking DOD IW capabilities when required. In IW campaigns where a more focused functional or geographical approach is better suited, this entity could support CCMDs operating under existing authorities by advocating for higher-level authorities from the POTUS or SECDEF when needed. In comparison to a CCMD, the smaller size of this or-

ganization would also allow it to colocate with the rest of the whole-of-government IW organization to ensure appropriate coordination. Each functional and geographic combatant command, and each service component, could also supply IW liaisons to this organization and ensure efforts were coordinated, command interests were met, and that OIE are synchronized, coordinated, and deconflicted with other CCMD operations and activities the services undertake.

This whole-of-government organization, staffed with experts from independent USG organizations, the DOS, and the DOD, would become the US OIE's epicenter. This organization would provide the US the capability to counter complex IW campaigns, to proactively shape the IE, and protect its citizens and interests across the world.

Conclusion

Our adversaries are waging IW against US citizens—their efforts are complex, widespread, and effective. The PRC's uncontested ability to maneuver in the IE increased the challenge of combating COVID-19. In the early stages of the pandemic, the PRC sowed confusion regarding the nature of the virus, attempted to promote their own response while discrediting the response of its competitors, and blamed the US to reduce the negative effects to their global reputation. The cost of these actions is a contributing factor to the US losing more lives to the virus than the combined deaths of the Vietnam War and European theater in World War II, creating a risk of a deep economic recession and amplifying distrust between US leaders and its citizens.

If the proposed organization were in place before the COVID-19 outbreak, the USG could have more quickly identified the PRC's attempt to suppress information regarding the transmissibility of COVID-19. This information could have better informed the WHO and governments around the world regarding the severity of the virus, prompting earlier action. Additionally, this whole-of-government agency could have quickly leveraged interagency IW capabilities to engage in the fight earlier with greater impact than what occurred.

The proposed whole-of-government construct reinstitutes and resources an organization similar in scope to the USIA with various IW capabilities either falling under this organization or directly partnering with it. Such a structure, empowered with the resources and authorities necessary to meet the scope of today's threats, could provide the US a better capability to counter complex IW campaigns, more proactively shape the IE, and better protect its citizens against adversaries waging IW. Most importantly, this structure would provide a central organization purposefully designed and equipped to use information as an instrument of national power, filling in a current gap of US capability.

The benefit from this organization is the development of the necessary expertise, depth of analysis, and continuity to take a long-term approach to shaping the IE—much like our adversaries are already doing. Additionally, this whole-of-government organization would make cross-department planning groups for OIE standard practice and ensure all capabilities across the USG are considered during planning and engagement activities. Finally, this organization, empowered with tasking authority, could simplify the complex authorization process, ensuring the right authorities are delegated to the right entity early enough in a campaign to bring the USG's full capabilities to action.

While COVID-19 was used as an example of IW, these tactics continue to be applied to shape the IE to support strategic objectives. Adversaries such as Russia and Iran have engaged in IW aimed at causing confusion, sowing distrust, and shifting blame in a variety of political, military, and economic situations. Even when the world recovers from COVID-19, the US will remain entrenched in great-power competition, and adversaries will continue to exploit the US inability to compete in the IE to further their strategic objectives. ✪

Capt Anthony J. Eastin, USAF

Captain Eastin (BA, BS, University of Nevada Las Vegas; MS, Bellevue University; MS, George Washington University) is the intelligence flight commander to the 57th Information Aggressor Squadron at Air Combat Command, US Air Force, Nellis AFB, Nevada. He previously served as the deputy chief to the information warfare branch at US Air Forces in Europe/Africa A39, where he would characterize the information environment to understand adversary tactics, techniques, and procedures, provide the Combined Forces Air Component Command with recommendations on how to operate in the information environment, and helped to pave the way for US Air Force information operations in Africa.

1st Lt Patrick G. Franck, USAF

Lieutenant Franck (BS, United States Air Force Academy [USAFA]) enlisted in 2012 as a scientific application specialist and received an appointment to the USAFA. Upon graduating, he entered the information operations career field and served in the US Air Forces in Europe/Africa A39 as the major command deputy operational security program manager and information warfare analyst. While serving at the A39, he was also attached to Joint Task Force (JTF)-Israel as the primary information environment analyst to advise the JTF commander. While working with JTF-I, he developed a joint US and Israeli Defense Forces method to merge operational security practices for the JTF.

Notes

1. World Health Organization, "Rolling Updates on Corona Virus Disease (COVID-19)," 17 May 2020. https://www.who.int/.
2. Susan V. Lawrence, "COVID-19 and China: A Chronology of Events (December 2019–January 2020)," *Congressional Research Service*, 13 May 2020, https://crsreports.congress.gov/.
3. Lawrence, "COVID-19 and China."
4. Lance Lambert, "The Coronavirus Has Now Killed More Americans Than the Vietnam War, Gulf War, Afghanistan War, and Iraq War Combined," *Fortune*, 15 May 2020, https://fortune.com/.

5. Department of Defense Instruction 3608.11, *Information Operations Career Force*, 4 November 2005, https://www.esd.whs.mil/.

6. Gregory R. Copley, "Beijing's 'Unavoidable' War: The 21st Century's Total War Has Begun," *Defense & Foreign Affairs Strategic Policy*, 6 May 2020, 4–9; and Qio Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: Peoples' Liberation Army Literature and Arts Publishing House, 1999).

7. Anthony J. Eastin, and Patrick G. Franck. "Information Warfare on United States' Citizens: How China Weaponized COVID-19," *OTH Journal*, 27 August 2020, https://othjournal.com/.

8. Lawrence, "COVID-19 and China."

9. Lawrence, "COVID-19 and China."

10. Lawrence, "COVID-19 and China."

11. Shan Li, "China's Internet Users Foil Censors to Keep a Wuhan Doctor's Interview Online," *Wall Street Journal*, 13 March 2020, https://www.wsj.com/.

12. Andrew Green, "Li Wenliang," *The Lancet* 395, no. 10225 (18 February 2020): 682, https://doi.org/.

13. Jun Feng and Guodong Liu, "8 People Were Dealt with in Accordance with the Law Because of Dissemination of False Information about 'Wuhan Viral Pneumonia' on the Internet," *China Court*, 1 January 2020, https://www.chinacourt.org/; and "China: 8 People Spread 'Wuhan Pneumonia' False Information Was Processed," *Xinhua News Agency*, 1 January 2020, https://crofsblogs.typepad.com/.

14. Liu, "8 People Were Dealt"; "WHO Timeline—COVID-19," *World Health Organization*, accessed 21 May 2020, https://www.who.int/.

15. World Health Organization, "Preliminary Investigations Conducted by the Chinese Authorities Have Found No Clear Evidence of Human-to-Human Transmission of the Novel #Coronavirus (2019-NCoV) Identified in #Wuhan, #China. Pic.twitter.com/Fnl5P877VG," *Twitter*, 14 January 2020. https://twitter.com/.

16. Jeremy Page, Wenxin Fan, and Natasha Khan, "How It All Started: China's Early Coronavirus Missteps," *Wall Street Journal*, 6 March 2020, https://www.wsj.com/; and Chaolin Huang et al., "Clinical Features of Patients Infected with 2019 Novel Coronavirus in Wuhan, China," *The Lancet* 395, no. 10223 (15 February 2020): 497–506, https://doi.org/.

17. World Health Organization, "COVID-19 Main Data Page," 29 July 2020, https://www1.nyc.gov/.

18. World Health Organization, "WHO Coronavirus Disease (COVID-19) Dashboard."

19. BBC News, "Coronavirus: China Outbreak City Wuhan Raises Death Toll by 50%," *BBC News*, 17 April 2020, https://www.bbc.com/.

20. Dr. Derya Unutmaz, "Seasonal Flu until: 2020-01-31 since: 2019-12-01—Twitter Search," *Twitter*, 23 January 2020, https://twitter.com/.

21. Emily Feng, "How China Uses Twitter and Facebook to Share Disinformation About Hong Kong," *NPR*, 20 August 2019, https://www.npr.org/.

22. Feng, "How China Uses Twitter and Facebook"; and Lijian Zhao, "7. Chinese Spokesperson: US Flu from 2019 to 2020 Has Caused 19 Million Infection Cases & at Least 10,000 Deaths. By Contrast, by February 2, 17,205 Cases of 2019-NCoV Pneumonia Were Confirmed, 361 Died & 475 Cured & Discharged, While There Are Only 11 Confirmed Cases in the US," *Twitter*, 3 February 2020, https://twitter.com/.

23. Bianji Liang Jun, ed., "Japanese TV Report Sparks Speculations in China That COVID-19 May Have Originated in US," *Global Times*, 23 February 2020, http://en.people.cn/.

24. Tanner Brown, "Inside China's Campaign to Blame the U.S. for the Coronavirus Pandemic," *MarketWatch*, 15 March 2020, https://www.marketwatch.com/.

25. Huileng Tan, "Beijing Objects to Term 'Wuhan Coronavirus,' and Says It May Not Have Originated in China," *CNBC*, 10 March 2020, https://www.cnbc.com/.

26. *CGTN*, "Xi Says China Ready to Help South Africa Fight COVID-19," 8 April 2020, https://news.cgtn.com/.

27. *CGTN*, "Xi Says China Ready to Help."

28. World Health Organization Situation Report, "Novel Coronavirus (2019- nCoV: Situation Report 13," 2 February 2020), https://www.who.int/.

29. Saranac Hale Spencer, "Conspiracy Theory Misinterprets Goals of Gates Foundation," *FactCheck.org*, 14 April 2020, https://www.factcheck.org/; John Yang, Sam Lane, and Mike Fritz, "The Dangerous Global Flood of Misinformation Surrounding COVID-19," *Public Broadcasting Service*, 28 April 2020, https://www.pbs.org/; and Jason Slotkin, "Birx On 'Stay-At-Home' Protests: 'Devastatingly Worrisome,'" *NPR*, 3 May 2020, https://www.npr.org/.

30. See the *Joint Concept for Integrated Campaigning* for a description of the conflict continuum used in this article.

31. Jeffrey V. Dickey et al., "Russian Political Warfare: Origin, Evolution, and Application," Naval Postgraduate School thesis, June 2015, https://calhoun.nps.edu/.

32. US Department of State Office of the Historian, "185. Report Prepared by the National Security Council," accessed 22 May 2020, https://history.state.gov/.

33. *Federal Register*, "Agencies—Broadcasting Board of Governors," accessed 22 May 2020, https://www.federalregister.gov/.

34. United States Agency for Global Media, "Budget Submissions," accessed 22 May 2020, https://www.usagm.gov/.

35. Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States*," 25 March 2013. https://www.jcs.mil/.

36. The authors have experienced this firsthand in large-scale multiple CCMD exercises.

37. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, 16 March 2018, https://www.jcs.mil/.

38. The DOD recognizes this issue. See the *Joint Concept of Integrated Campaigning* for a description of this continuum.

39. 2 FAH-2 H-110 Post Management Organization, "Chief of Mission Authority, Security Responsibility, and Overseas Staffing," https://fam.state.gov/.

40. US Code Public Law 114-328, Section 1287, 23 December 2016, *Global Engagement Center*, https://uscode.house.gov/.

41. US Code Public Law 114-328, Section 1287.

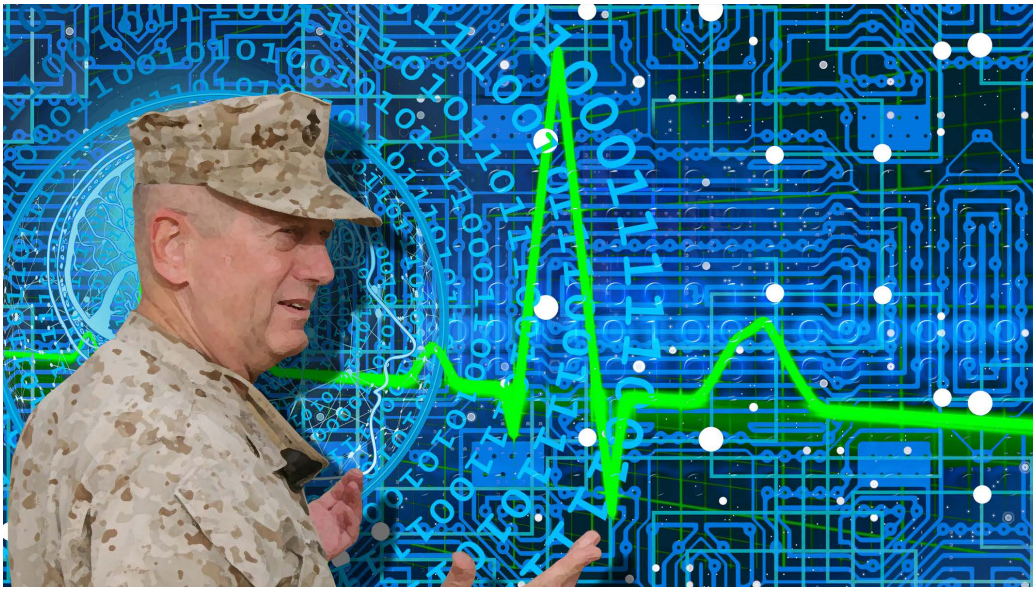
42. Conrad Crane, "The U.S. Needs an Information Warfare Command: a Historical Examination," *War on the Rocks*, 14 June 2019. https://warontherocks.com/.

FEATURE

Information Warfare

Tuning Our Instruments to Overcome Barriers to Battlefield Harmony

Col Nathaniel Huston, USAF
Capt Keegan Newton, USAF
Capt John Runge, USAF



Introduction

I don't care how operationally brilliant you are; if you can't create harmony—vicious harmony—on the battlefield, based on trust across different military services, foreign allied militaries, and diplomatic lines, you need to go home.

—Gen James Mattis

Battlefields are complex places, as Gen Mattis so eloquently pointed out in his recent memoir, *Call Sign Chaos*. Though the former defense secretary was reflecting specifically on the trust built between commanders in the run-up to *Operation Iraqi Freedom*, he rightly observed that the need for trust extends to all levels and forms of war fighting. Each pilot must trust his wingman, each soldier must trust his squad members, each commander must trust her fellow commander. Similarly, force employers and enablers must build trust between other employers and enablers. The bomber pilot must trust the targeteer to mensurate an aim point with precision, the fighter pilot must trust the tanker will fill her aircraft with nothing

but the highest quality jet fuel, and the logistician must trust that the defender will keep his base safe. War fighting, quite simply, is an exercise in trust.

Today's war fighters face especially acute and compelling challenges regarding trust building. Similar to their forebears of 100 years ago—when the world's militaries grappled with how to effectively integrate war fighting from and through a new air domain—today's Airmen, Soldiers, Sailors, and Marines must compete on a battlefield altered by the introduction of an unfamiliar new domain, one that can be hard to conceive of, let alone integrate with. Recognizing this challenge, the US military has, during the past decade, significantly increased its institutional and operational capabilities in cyberspace and across the information warfare (IW) landscape.[1] One need look no further than the designation of US Cyber Command as our nation's 10th combatant command, for example, as a signal of the importance placed on the new domain.

Be that as it may, new organizations are not, by themselves, enough. To achieve the full potential of emerging technologies and fully exploit this new domain, warfighters on both sides of the digital divide must fundamentally adapt the ways in which they exploit their warfighting means. Simply employing new technology is not enough; the organization itself must change how it approaches the battlefield if it is to have success upon it. Today's warfighters face an inflection point, one in which trust plays a pivotal role. To borrow a phrase from our special operations brothers and sisters, for the US to be successful at operating *by, with,* and *through* the information environment, we must intensify integration efforts and eliminate barriers that prevent building the trust necessary for the vicious harmony we seek to achieve.

This article argues there are three primary barriers that prevent the effective integration, synchronization, and convergence of IW capabilities with each other and, perhaps more importantly, with the broader spectrum of multidomain capabilities. First, IW integration is hampered by the lack of a common lexicon, both within and between IW functions and between IW and other war-fighting elements. This not only prevents efficient internal and external synchronization but also obscures how IW complements full-spectrum operations. Second, IW suffers from a tendency to over-classify information that prevents operational decision-makers from understanding, integrating, and leveraging IW capabilities. Finally, although progress has been made, authorities to employ IW capabilities are still widely held at high levels that inhibit war fighting agility and diminish the potential impact of these capabilities. Many seek the path to the successful integration of our disparate IW functions and further, to their integration and synchronization with the broader spectrum of military capabilities; breaking down these barriers promises to accelerate this vision's timeline.

Indeed, following that path and achieving vicious harmony is critical on today's battlefield, one that remains increasingly interconnected through the advancement and employment of information technology. In today's information age—where war fighters are surrounded by screens, sensors, control devices, and signals—trust and harmony are crucial to success. Whether in the avionics back shop of an F-15 hanger, accessing Predator feeds from a handheld Rover device, or monitoring network operations on a standard Windows workstation, cell phones, smart watches, and computers abound. These devices are sending and receiving signals almost without stop. Although technology has provided increased work capacity and convenience, it also introduced a new contested domain that can be exploited for warfighting purposes. Our adversaries have already begun to capitalize on the potential for military operations through the information environment and are actively developing strategies to take advantage of it.[2] To maintain (or as some have argued, regain) a position of relative advantage, the United States must make every effort to maximize the unified potential of cyberspace operations (CO), information operations (IO), electronic warfare (EW), and intelligence, surveillance, and reconnaissance (ISR).[3]

With respect to our argument, it is with these information-related capabilities (IRC) that we wish to spend the most time in contemplation below. Relative to IRCs, "traditional" military capabilities—those that exist mostly in the physical dimension—tend to be easier to trust, most simply because they are easily perceived by our senses.[4] One can hear and feel the roar of an F-22 as it conducts a defensive counterair sortie. One can see the "boots on the ground" of the soldier occupying enemy territory. IRCs on the other hand, have yet to earn the same level of operational trust.

IRCs can be difficult to understand, and their accesses and effects are often plagued by increased uncertainty relative to their often more explosive counterparts. They are rarely visible to the human eye, requiring instead the interpretive lens of a workstation. Their ethereal nature often means that earning trust is an inherently uphill battle. It is all the more imperative, then, that to the extent possible, barriers preventing harmony be removed. The first barrier, which prevents effective communication, is perhaps the most basic but also most challenging to overcome. Absent a common lexicon, IW operators often struggle to communicate with each other, let alone with those outside the virtual world in which they travel. This situation hampers their own understanding of how they fit within the overall mission and often hinders "outsiders" from accurately perceiving the reality of what the IW community has to offer.

Barrier One: Communication

Many readers are likely familiar with the old trope that goes something like, "communicators are the worst at communicating." Long have the so-called computer nerds of the military suffered the ill effects of "tech-itis," chief among them the peculiar malady of a vocabulary increasingly consisting of beeps and squeaks. This situation can be expected, to some extent, as any profession naturally develops a distinct vocabulary, a shared language of implicit meaning, and shortcuts allowing efficiency of communication. IW career fields are no different; as they evolve, they naturally develop a language that allows them to more effectively communicate within the ones and zeros of the information environment. Just as pilots have developed an understanding of their domain and concomitant vernacular, cyber operators—as they have professionalized and come to understand the information environment—have developed their own language of operations. While this is to be expected, and indeed even celebrated as the career field matures, it offers challenges that, if not addressed, promise to hinder trust, integration, and, ultimately, battlefield harmony. The lack of a common lexicon impedes integration among IW providers, frustrates their ability to understand how they fit within the multidomain fight, and finally, can lead to their exclusion from without, as others struggle to perceive their value to the joint fight.

First and most fundamentally, a new lexicon is only useful to the extent that it is a *common* lexicon. Although many of the beeps and squeaks of the cyber environment are similar, their operationalization can tend to constrain practitioners in silos of self-identification that separate them from the war fighting identity they share with their fellow men and women in uniform. This is of course true in any military domain; as Sun Tzu reminds us, knowing one's enemy is critical to success on the battlefield. Sun Tzu also counsels, however, that one must also know oneself, and in an environment in which war fighting looks so different, the importance of common language is heightened. CO tends to live within organizational constructs and use naming conventions that reflect their unique relationship within the information environment. Roles include technical directors and exploitation leads, each of which have specific roles and responsibilities to the mission.[5] EW, on the other hand, organizes its operations in the electromagnetic spectrum around the concepts of electromagnetic attack, electromagnetic warfare support, and electromagnetic protection.[6] IO offers yet another conceptual framework from which to perceive operations in the information environment, referencing "actions taken to affect adversary information and information systems while defending one's own information and information systems."[7] Understanding how these concepts relate to and differ from one another is critical to integrating their effects against an ad-

versary and is not easily accomplished between the IW functions themselves, let alone between IW functions and the larger joint force.

To be sure, there is a place for specialized and precise lexicon. Within the context of IW, however, the independent growth of this myriad of functions has led to a panoply of vocabularies that make communicating between them difficult, leading to a second and equally concerning challenge. Without a common lexicon, it can be hard for IW practitioners to understand their place within their own service or the larger joint mission. A common lexicon can help to define not just one's own processes and identity but how that identity fits within its larger organization.

The Marine Corps Planning Process, for instance, helps unify Marines around a common concept of maneuver warfare.[8] Whether driving a tank, flying a helicopter, or storming a beach, a Marine's place within the Marine Air-Ground Task Force (MAGTF) is defined by his relationship to his fellow Marines and as such, to the larger joint force. Marines are taught from an early point in their careers how the functions of the MAGTF work together in a synchronized and integrated way. Similarly, military aviators share a common language and lexicon while still specializing in—and speaking about—their own specific weapon systems in unique terms. Simply put, these communities have professionalized their approach to war fighting individually but also collectively. We cannot yet say the same of those operating within the IW environment.

As IW advances and the entire community professionalizes, practitioners across the various functions must undertake to find common ground and institutionalize their approach, just as any professional community would. To the extent possible, the community should seek to integrate its own language and practices into those of their joint partners. "Dropping cyber bombs" may be an unhelpful and perhaps unfortunate euphemism, but one need not throw the baby out with the bathwater when it comes to integrating and normalizing language.[9] Concepts like joint fires, movement and maneuver, and protection certainly might not map as precisely onto the information environment as they do to physical realm, but they are doctrinal and, most importantly, shared. These terms allow war fighters to communicate between and across functions, which provides tighter integration and synchronization. A concerted effort to create a common vocabulary and fit it within these shared concepts is a good way to professionalize within IW and maximize its potential within the joint force.

To some extent, the stand-up of Sixteenth Air Force (Sixteenth AF) has begun to alleviate this challenge—for the Air Force at least—by offering those within it a single organization from which to derive their identity and, as such, comprehend their position within the larger war-fighting construct. In a recent interview General Haugh, the first and current commander of the newly activated Sixteenth

AF, referenced the need to integrate these disparate functions as the impetus of the organization's creation.[10] As the organization matures, it will be important for its members to conceptualize not just how they relate to others within the IW community but also how they all fit into the larger organization of the US Air Force and indeed, the entire joint force. This is all the more imperative for those operating within the information environment, where self-imposed boundaries between services quickly fade away from an adversary's perspective. A common lexicon among and between IW professionals will help sharpen their perception of where they fit and facilitate synchronization of effects across the spectrum of operations, allowing the whole to become greater than the sum of its parts and invigorating the trust upon which victory on the battlefield must rest.

In addition to a sharper self-perception, this foundation is crucial to build "outside-in" trust; that is, trust *from* outside of the IW community *in* what the IW community has to offer. Sixteenth AF offers those within it a shared identity but from the outside, Sixteenth AF is a lot of things to a lot of people. In the same interview, General Haugh referenced no fewer than 10 significant and wide-ranging missions for which he is responsible.[11] In many ways, what IW means to an individual is derived from where that individual sits organizationally and what slice of IW is most significant to that organization, which leads to the final challenge facing an IW community without a common lexicon: without the ability to speak the same language, IW operators struggle to speak with a single voice and, as such, struggle to communicate their value to the larger joint force. This is not to say that they are *un*valued, but simply that when IW is so many things to so many people, it can be hard to accurately perceive its full potential when properly integrated.

Here again, the stand-up of a consolidated organization in the Air Force offers a promising first step to helping "outside" customers recognize how IW functions fit within the larger range of military operations. ISR capabilities, for instance, have progressively become more assimilated across all mission types. Full-motion video has become an almost-expected commodity among war fighters across the services, and battle damage assessments, always critical to determining the effectiveness of a given operation, have become tightly integrated throughout the joint force. As those functions have matured, their lexicon has matured to communicate effectively and efficiently with joint partners to enable a level of synchronization not as widely enjoyed across the rest of the IW spectrum. Learning from this example and building on this strength will help elucidate the value the entire IW community brings to the joint fight.

Barrier Two: Classification

Sun Tzu counsels, "Conceal your dispositions, and your condition will remain secret, which leads to victory; show your dispositions, and your condition will become patent, which leads to defeat."[12]

Today's information environment is nothing if not Sun Tzuian, at least in this respect, perhaps to a fault. Although well-intentioned, many operating within the domain suffer from a predisposition to protect rather than share, which has resulted in an environment of over-classification that threatens to undermine the effectiveness of the very systems we seek to protect.[13] This is understandable, of course. From very early in their careers, war fighters privy to classified information are correctly trained that security of resources, access, sources, and information is paramount to operational security. Vigilance, in protection and secrecy, is critical to the preservation of the nation's technological edge and position of strategic advantage, such that those exist. Those with security clearances are keenly, and appropriately, aware of the repercussions of under-classifying material—both from an operational standpoint and a personal standpoint. Risk must not be taken unnecessarily.

War fighting, however, involves risk, at least to some extent. There is a cost to "playing it safe" and erring on the side of caution. Over-classification of material not only erodes public trust in military processes and costs an estimated amount of billions of dollars every year, but hinders effective war fighting.[14] This is especially true in the information environment. If mission partners within and external to the IW community cannot access critical information due to over-classification, IRCs cannot be effectively and harmoniously integrated into the twenty-first century battlespace. IW becomes a victim of its own sensitivity.

This is not, of course, a problem unique to the IW community. General John Hyten, the vice chairman of the Joint Chiefs of Staff, told the audience at an Air Force Association event that "in many cases in the department, we're just so over-classified it's ridiculous, just unbelievably ridiculous." General Hyten related a story in which, when he was head of US Strategic Command, he invited the then-head of US Pacific Command, Adm Harry Harris, to a briefing that was so classified, even their deputy commanders, both three-star flag officers, were not allowed in the room.[15] General Hyten lamented that if "the only people in the room are four-stars, you really can't get any work done."[16] His point, and the point of our own argument, is that classification of information always involves weighing risks and rewards; it involves tension between safeguarding information from the enemy and ensuring the right information gets to the right people to prosecute the enemy. The challenge is ubiquitous in the IW environment.

Similar to the first barrier, the over-classification barrier is inherently a communication challenge that has the potential to impact successful mission execution. How can planners practically integrate IRCs without fully understanding those capabilities or, at a minimum, the basics of how they work, their effects, and their dependencies? The bulk of today's operational planning and execution occurs at the Secret level. Most of the capabilities that planners consider for air and ground operations can be found on unclassified or Secret-level networks. This gives all planners the opportunity to understand these capabilities and build a plan around them. This is not the case with IW capabilities, which are usually not only highly classified, but also often require special accesses. The negative effects of over-classification manifest at the tactical, operational, and strategic levels, but at the lowest levels, integration is significantly hindered by the inability to share during operational planning.

In addition to its negative impact on planning, over-classification negatively impacts the potential of the IW community to earn operational trust. If fellow war fighters are not given enough information to understand various IRCs, trust is very difficult to gain and, along with it, the effective utilization of those capabilities on the battlefield. In the absence of confidence in IW capabilities, war fighters understandably default to traditional military capabilities, those they can feel and hear and whose effects are directly observable once the smoke clears. Without trust, IW operators risk handicapping their own effectiveness. In a business in which effectiveness is often measured in lives lost, these costs are simply too great to bear unnecessarily.

The good news is, in this challenge IW professionals are not alone. The space community, for instance, has long faced a similar challenge of trying to integrate highly classified capabilities. Information about these capabilities must be protected to prevent undermining their operational effectiveness, but leaders within what is now the US Space Force have recognized the need to empower their operators in order to improve war-fighting efficiency, which required communication lines to be less restricted. To achieve this, leadership probed the issue from several angles. What information can be made unclassified? What information can be made nonprogram classified? And, instead of single-access programs, could umbrella-access programs be created? With these questions in mind, and the understanding that an inability to adapt would cause continued inefficiencies and the potential for adversarial surprise, the space community has made progress on loosening classification restrictions.[17] Unsurprisingly, this change has been a catalyst to better enable the joint force to integrate its arsenal of capabilities.[18]

The IW community faces similar challenges. How can IW practitioners effectively communicate and work with the joint force if they are not able to access IW

resources at the places where the fight occurs? The issue is being addressed, and the Chairman of the Joint Chiefs of Staff has directed a re-evaluation of our classification guidance.[19] In the meantime, IW planners might help by creating an IW playbook (a database of sorts) containing summaries of existing capabilities that is accessible at the Secret level and across the operational community. This repository could also list "best practice" integration techniques across the spectrum of IW capabilities. It could, for example, explain how ISR could be leveraged to work in concert with CO to deny an adversary's access to a given communication link or platform while at the same time using IO to create a leaflet campaign telling civilians to not use that link or platform. If such a repository currently exists, institutionalization of its use across the joint planning enterprise could increase its usefulness.

Gen Mattis once suggested that he had "never been on a crowded battlefield, and there is always room for those who want to be there alongside."[20] Ultimately, sensitive information must be protected, but in a manner that allows cooperation among and between mission partners. If classification decisions come at the expense of military progress and dominance in IW, they must be made deliberately and with the knowledge that they come at a real cost. Military members, even those operating in the virtual battlespace, are in the business of fighting wars, and war fighting involves risk.

Make no mistake, the argument is not to lower classification levels across the board. Rather, the intent is to arm commanders and planners with an increased knowledge of how IW capabilities can be integrated into the fight. Ultimately, the desire is to pave the way for expanded knowledge at lower levels for increased authorities to be delegated. Expanded knowledge of capabilities paves the way for increasingly informed and deliberate decisions regarding risk that are able to be made at progressively lower levels—levels that cannot today be trusted to make informed decisions often because they have no knowledge of the capability itself, let alone risk associated with employing it. As we give a little in making the knowledge of these capabilities available at a lower classification level, we gain a little in the way of trust by the joint force.

Barrier Three: Authorities

The final barrier at issue is one near and dear to many cyber operators' hearts. Seemingly since the first bit was fired in anger, many have lamented what they perceive to be an overly-restrictive approach to employing cyber capabilities, one that holds authorities at a level so high as to prevent many operations from being executed in a timeframe short enough to be effective.[21] Those familiar with the debate, of course, will know that there are very good reasons for the seemingly

overly-restrictive approach. Often, decision-makers must decide whether the benefit from an operational effect outweighs the potential benefit of continued access to a given source of intelligence.

Additionally, there are very real legal issues that remain unresolved regarding where to draw the line between Title 10 and Title 50 actions when it comes to operations in cyberspace.[22] Further, IRCs are often costly to develop in terms of access, time, and money. Regardless of any debate about continued intelligence exploitation, simply using a given capability can highlight a vulnerability, thus nullifying the IRC's potential for future effects and therefore increasing the "per unit" cost of the weapon exponentially. Finally, given the nature of the information environment, operations in cyberspace offer exponentially higher risk posed by what has come to be known as the "strategic corporal," a war fighter who, though operating at a tactical level, may have strategic and political effects. While many in the US military have recognized and actually begun trying to leverage this new reality, the nature of operations in cyberspace remain at risk of resulting in outsized and unintended effects and as such, trepidation remains with regard to pushing decision-making lower in the chain of command.[23]

Suffice to say, there are many good and just reasons to keep a wary eye on efforts to increase authorities at lower levels. Today's cyber warfare landscape, however, suggests that there are good reasons to take increased risk in this arena. The doctrinal emphasis China places on seizing the initiative as the "single most decisive factor in controlling and winning a war," or the extent to which Russia values swift actions during the Initial Period of War echoes the need to make decisions at an increased pace.[24] These sorts of challenges are not unique to IW, and we would be well-served to look to other force employment platforms to learn how to loosen restrictions and increase agility at lower levels while continuing to maintain a healthy respect for the risks incurred by doing so.

In the case of air warfare, for instance, a combatant commander carries the ultimate responsibility of calling strikes in his or her theater, but operationally pushes strike decision authorities lower down, to the battle director, at an air operations center. The intent is to shorten the kill chain, the process of rapidly understanding threats, making decisions, and taking military actions.[25] At times, even this chain of approval has proven too cumbersome for effective, "harmonious" combat operations. Facing real challenges with coordinating time-sensitive strikes on emerging targets, innovative air strategists in the 1980s developed what would become known as "kill boxes," essentially pre-coordinated three-dimensional areas wherein authorities to strike targets were pushed to a lower, more tactical level. Importantly, they were not conceived of as "free fire" zones, but were instead intended to be areas in which the rules of engagement were deliberately and pur-

posely tailored to allow decision-making to proceed at a more rapid pace.[26] Today, the concept is enshrined in doctrine and is a standard part of the toolkit available to commanders and planners seeking to increase dexterity and empower war fighters to make time-critical, risk-informed decisions in the heat of battle.

Whither IW's "kill boxes?" What innovative solutions might the joint force be able to offer to mitigate the risk of unintended consequences while acknowledging the real need to increase agility on the part of cyber operators making split-second decisions and executing operations that at times quite literally occur at the speed of light? The importance of empowering war fighters at the operational and tactical levels is hard to overestimate. Gen David Goldfein, former USAF chief of staff, in fact, made revitalizing the squadron a centerpiece of his strategic vision.[27] In eliminating costly red tape in its processes and removing hundreds of outdated or frivolous instructions, Air Force leadership has liberated its war fighting force and pushed authorities down to lower levels, thus creating an environment more suitable to a shortened kill chain.[28] National Security Presidential Memorandum 13, signed in August of 2018, appears to be a good first step to loosening the reins in cyberspace.[29] It pushes authorities to lower levels and allows for a significant increase in the number of operations, but more work remains to be done to allow dexterity and synchronization while providing assurances that oversight will remain effective.[30] One process-related solution is the concept of a selection of Pre-Approved Actions (PAA) that enable commanders to take rapid, decisive actions on the battlefield in response to specific operational events or "triggers." This solution has begun to find its way into other areas of IW such as CO, but the capability is nascent and its future uncertain.[31] In any case, whether through virtual "kill boxes" or an invigorated approach to PAAs, IW requires innovation to allow the sort of increased, deliberate risk-taking that will increase agility and synchronization throughout the information environment.

Conclusion

We cannot know the way if we do not see the path. These barriers represent restrictions that create friction as we strive toward synchronization, integration, and ultimately, vicious harmony between the rapidly growing IW battlefield and the broader environment of military operations. For IW operators to breach these barriers, the Department of Defense (DOD) must take a serious look at the culture that has grown around the information environment of warfare. IW should focus specifically on identifying the ways in which commanders can be effective at delivering IW capabilities. In the DOD, we have initiatives to increase our ability to conduct IW by combining the effects of EW, IO, CO, and ISR in new and exciting ways. While the future state of synchronized, converged, and inte-

grated IW capabilities is invigorating, we must first deal with our self-imposed, internal barriers to a successful campaign in the information environment.

There are three primary obstacles preventing achievement of the desired IW future state. First, IW practitioners have experienced difficulties in understanding the battlespace and lexicon within our own communities and those of the joint force, which has resulted in communication challenges, both internal and external to the IW community. Second, IW capabilities are frequently highly classified, which makes mission planning difficult, especially across a multidomain operation. If members across the planning process are not knowledgeable of a particular program or capability, decision-makers are understandably handicapped, and operations are potentially less effective. Third, although we are making progress pushing authorities to lower levels, more must be done to offer commanders creative ways to allow lower-level decision-makers the authority they need to become more agile. These barriers stand in the way of creating the vicious harmony necessary to maximize the potential offered via operations *by, with*, and *through* this new domain.

To overcome these barriers, we must aggressively push forward on several fronts. First, IW professionals ought to work hard to establish a common lexicon that will both increase their own understanding of how they fit into the larger war fighting effort and allow those outside the community to understand the value their capabilities offer. Further, leadership must continue to critically examine the risk versus reward of current classification requirements and their impact on our national defense. Simply put, IW dominance requires a more widespread understanding across the spectrum of planning and decision-making. This understanding can only be accomplished through making deliberate and informed decisions about where classification requirements can be relaxed. Finally, to match the speed at which war fighting can occur in cyberspace, operational and force employment decisions must, to the greatest extent possible, be pushed lower in the chain of command.

Importantly, much of what is advocated for above involves building a culture inside of IW that is comfortable with increased risk. Equally as important, the risk must not be unmitigated but rather deliberate and thoughtful. To the extent that victory upon today's battlefields hinges on America's ability to leverage IW capabilities more effectively than her adversary, we argue that the increase is justified. In order to capture significant technical gains, an organization must reward successful risk-taking and minimize penalties for failure. Unwillingness to take risk should be eschewed altogether.[32] In shaping our future, we should look to the examples of our fellow war fighters, those who have fought successfully for de-

cades on land, air, and sea. We must professionalize, take risk, and build trust in order to achieve vicious harmony on tomorrow's battlefields. ✪

Col Nathaniel Huston, USAF

Colonel Huston (BS, MA, PhD, University of Notre Dame; MS, Air Command and Staff College; MPhil, School of Advanced Air & Space Studies) is a School of Advanced Air and Space Studies professor of strategy and security studies.

Capt Keegan Newton, USAF

Captain Newton (BA, BA, Virginia Polytechnic Institute and State University; MS, Iowa State University) is an operator on a Department of Defense Red Team.

Capt John Runge, USAF

Captain Runge (BA, University of Nevada, Las Vegas) is a 7th Intelligence Squadron assistant director of operations.

Notes

1. Sixteenth Air Force, "16th Air Forces (Air Forces Cyber)," 31 July 2020, https://www.16af.af.mil/.
2. Joint Publication (JP) 3-13, *Information Operations*, 20 November 2014, ix–x, https://www.jcs.mil/; and James Mulvenon and Richard Yang, *The People's Liberation Army in the Information Age*, RAND Report CF-145-CAPP/AF (Santa Monica, CA: RAND, September 1999), 175–86.
3. Dustin Weaver, "Lawmakers Fear US Has Fallen behind in Cyber Warfare," *The Hill*, 5 March 2017, https://thehill.com/; Peter Apps, "Commentary: As Cyber Warfare Turns 10, the West Risks Falling Behind," *Reuters*, 4 May 2017, https://www.reuters.com/; Gopal Ratnam and John Donnelly, "America Is Woefully Unprepared for Cyber-Warfare," *Roll Call*, 11 July 2019, https://www.rollcall.com/; Lawrence Sellin, "*The US Is Unprepared for Space Cyberwarfare*," *Military Times*, 4 September 2019, https://www.militarytimes.com/; JP 3-12, *Cyberspace Operations*, 8 June 2018, vii, https://www.jcs.mil/; JP 3-13, *Information Operations*, 20 November 2014, ix–x; JP 3-13.1, *Electronic Warfare*, 8 February 2012, v-vi, https://fas.org/; and JP 2-0, *Joint Intelligence*, 22 October 2013, I-11, https://www.jcs.mil/.
4. JP 3-13, *Information Operations*, ix–x.
5. Maryse Penny, Tess Hellgren, and Matt Bassford, *Future Technology Landscapes: Insights, Analysis, and Implications for Defence* (Washington, DC: RAND, 5 December 2013), 77–79.
6. Curtis E. LeMay Center for Doctrine Development and Education, "ANNEX 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operations," 30 July 2019, 20–26, https://www.doctrine.af.mil/.
7. Herb Lin, "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations," *Lawfare*, 27 March 2020, https://www.lawfareblog.com/.
8. Marine Corps Doctrinal Publications 1, *Warfighting*, 4 April 2018, 3–9, https://www.marines.mil/.
9. Brandon Valeriano, Heather Roff, and Sean Lawson, "Dropping the Cyber Bomb? Spectacular Claims and Unremarkable Effects," *Council on Foreign Relations*, 24 May 2016, ***https://www.cfr.org/***.

10. Mitchell Institute, "Aerospace Nation: Lt Gen Timothy Haugh, Commander, Sixteenth Air Force, AF Cyber, & Joint Force HQ-Cyber," 15 July 2020, *YouTube* video, 1:16:13, https://www.youtube.com/.

11. Mitchell Institute, "Aerospace Nation: Lt Gen Timothy Haugh, Commander."

12. Sun Tzu, *The Art of War*, https://suntzusaid.com/.

13. Patrick Eddington and Christopher Preble, "Bad Idea: Overclassification," *Center for Strategic and International Studies*, 6 December 2019, https://defense360.csis.org/; and Cathy Maus, "Office of Nuclear and National Security Information: History of Classification and Declassification," *Federation of American Scientists*, 22 July 1996, https://fas.org/.

14. Eddington and Preble, "Bad Idea: Overclassification"; and Maus, "Office of Nuclear and National Security Information."

15. Aaron Mehta, "Unbelievably Ridiculous: 4-Star General Seeks to Clean Up Pentagon's Classification Process," *Defense News*, 29 January 2020, https://www.defensenews.com/.

16. Mehta, "Unbelievably Ridiculous."

17. Nathan Strout, "Barretts, Rogers Consider Declassifying Secretive Space Programs," *Defense News*, 7 December 2019, https://www.defensenews.com/.

18. Nathan Strout, "Nominee to Lead Space Command Voices Support for Declassifying Space," *C4ISRNET*, 28 July 2020, https://www.c4isrnet.com/.

19. Mehta, "Unbelievably Ridiculous."

20. James Mattis, "Duty, Democracy and the Threat of Tribalism," *Wall Street Journal*, 28 August 2019, https://www.wsj.com/.

21. Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," 8 May 2019, https://www.fifthdomain.com/.

22. Robert Chesney, "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries," *Lawfare*, 12 April 2018, https://www.lawfareblog.com/.

23. Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," 8 May 2019, https://www.fifthdomain.com/.

24. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).

25. Eric Jacobson, "Sino-Russian Convergence in the Military Domain," *Center for Strategic & International Studies*, 22 March 2018, https://www.csis.org/.

26. JP 3-9, *Joint Fire Support*, 10 April 2019, A-9, https://www.jcs.mil/.

27. Gen David Goldfein, USAF, "CSAF Letter to Airmen," 9 August 2016, USAF, https://www.af.mil/.

28. Stephen Losey, "Air Force Cuts 226 AFIs in Latest Salvo Against Hated 'Queep,'" *Air Force Times*, 29 August 2018, https://www.airforcetimes.com/.

29. Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," *Fifth Domain*, 8 May 2019, https://www.fifthdomain.com/.

30. Mark Pomerleau, "DoD Cyber Ops Are Changing, and so is Oversight," *Fifth Domain*, 3 June 2019, https://www.fifthdomain.com/.

31. JP 3-12, *Cyberspace Operations*, IV-15.

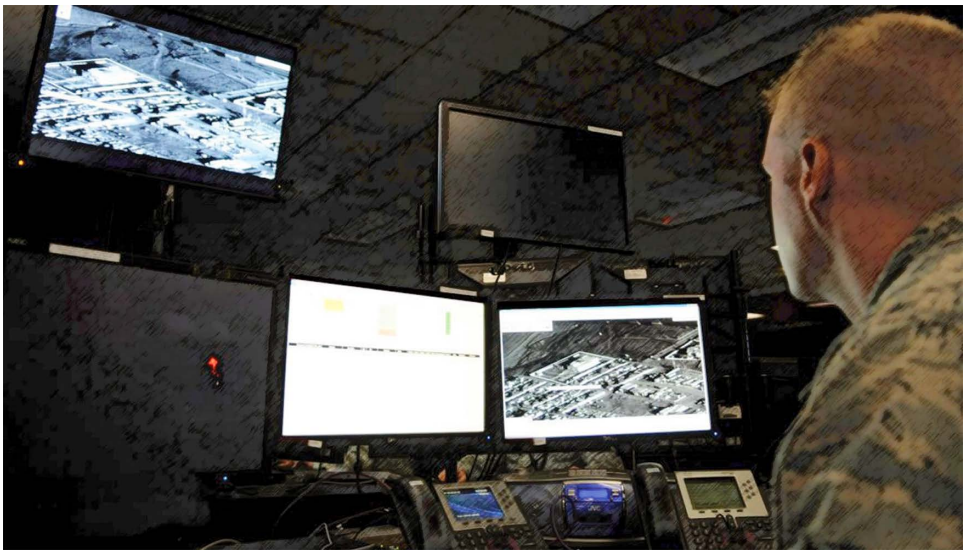
32. The Space Archive, "RAW Elon Musk Interview from Air Warfare Symposium 2020," 2 March 2020, *YouTube* video, 55:23, https://www.youtube.com/.

FEATURE

Empowering the Information Warrior

Unlocking the Latent Value of this Strategic Asset

Jay Fudemberg
Lt Col Robert D. Folker Jr., USAF, Retired



Purpose

Understanding one's adversary and generating deep insights about their intentions, capabilities, and actions is foundational for success in warfare.[1] As such, it is essential that the information warriors responsible for producing and acting on such intelligence have the necessary higher-order cognitive and critical thinking capabilities that will reliably generate the requisite understanding and insights. However, because of under-investment in the development of higher-order thinking and not having a structural means for systematically infusing these skills in intelligence operations, the Air Force is losing significant value that is essential for information warfare effectiveness.

This article will highlight a strategic opportunity, presently available, that will empower the Air Force to more effectively compete now by: (1) enhancing the higher-order and critical thinking capabilities of airmen, (2) infusing more robust insight generation capacity into information warfare processes, (3) better informing the war fighter to achieve desired outcomes, and (4) enabling the Air Force to converge the appropriate resources for managing escalation and solving problems in a timely fashion.[2] Toward these objectives, this article will describe a specific

platform that leverages human-machine teaming to enhance the higher-order cognitive capabilities of information warriors, unleashing their locked-up latent value and increasing their effectiveness. After introducing the issue, this article will address the following:

- Under-performance in higher-order thinking skills and processes (which includes critical thinking)
- Defining higher-order thinking skills and processes
- A strategic approach to developing, exercising, and assessing higher-order thinking
- A structural means for supporting and enhancing higher-order thinking by information warriors throughout their work activities

Introduction

A nation's ability to impose its will and achieve its desired objectives stems from its diplomatic, information, military, and economic instruments of national power (DIME).[3] While aspects of these four instruments of power are constantly in flux, information is increasingly important in the digital age.[4] Given information's ubiquity and growing importance, information warfare has also become omnipresent and prominent. Thus, information warfare has an essential role in serving to support and converge all instruments of power into a cohesive multidomain campaign.[5] And in doing so, it supports the *National Defense Strategy* goal of increasing the competitive space within which the US can shape the battlespace to the disadvantage of its adversaries.[6]

Accordingly, the Air Force is reinvesting in information warfare, after its initial attempt approximately 20 years ago. The Air Force recently restructured its separate Numbered Air Forces (NAF), the Twenty-Fourth Air Force (AF) and Twenty-Fifth AF respectively, into a single information warfare NAF, the Sixteenth AF, to unite its previously disparate efforts of cyber operations; electronic warfare (EW); information operations (IO); and intelligence, surveillance, and reconnaissance (ISR) into an integrated whole to influence its competitors' behaviors and deliver other desired outcomes throughout the entire spectrum of conflict.[7]

Due to the indispensable nature of information, intelligence, and decision-making to the success of warfare, it is essential to make intentional investments to not only develop the higher-order cognitive skills of information warriors but also to provide the structural means for systematically infusing these skills into intelligence operations. This is an immediate common-sense action that is possible with current technology and can yield a significant impact on information warfare.

The Information Warrior's Required Cognitive Abilities

Those responsible for conducting cyber operations, EW, IO, and ISR missions are the information warriors of this new era.[8] Though their expertise is varied, their effectiveness similarly depends upon the same foundation of higher-order thinking.[9] Specifically, these warriors should be able to:

- Identify the relevant aspects and elements of a problem
- Analyze the issue's scope, structure, elements, and dynamics
- Establish objectives
- Find connections and relationships between elements
- Construct meaning and understanding of the parts and the whole
- Find patterns and apply models
- Accurately infer all that is implied from what is known
- Uncover unknowns, ambiguities, and questions
- Reveal assumptions, biases, and falsehoods
- Formulate points of view and hypothesize alternatives
- Assess, evaluate, and judge the importance and probabilities of factors, criteria and points of view
- Reason logically and create well-reasoned fact-based arguments supporting the points of view
- Make decisions based upon the best available information, reasoning, and judgments

These skills are among the most important "elements of thought and reasoning" that are relevant to the information warrior.

Investing in Thought and Reason

While the US is advancing its information warfare capabilities, it is far from achieving information dominance. Much more can and must be achieved to increase the competitive space and maintain decision advantage. Although the Air Force invests significantly in generating, storing, and sharing information, it is not making adequate investments to ensure the systematic, comprehensive, accurate, and reliable creation of the "relevant elements of thought and reasoning" about the information. Surely, the "relevant elements of thought and reasoning" are as important as the underlying information in information warfare, if not more so, and as such, are worthy of serious investment.

Under-Performance in Higher-Order Thinking Skills

Only 6 percent of college graduates are proficient in critical thinking, according to the Educational Testing Service.[10] Seventy-five percent of employers find recent graduates deficient in critical thinking and problem solving, according to the American Association of Colleges and Universities.[11] These figures are just two of the many consistent statistics that indicate young people entering the workforce are poorly prepared for employment in areas requiring critical-thinking and problem-solving skills.

In the event the reader believes that the workforce within the Air Force fares better than the general population, the work completed by Col Adam "MEZ" Stone should dispel that illusion. Colonel Stone was able to measure the critical thinking ability of Airmen using a standardized exam, the Watson-Glaser Critical Thinking Appraisal (WGCTA). The test was comprised of 40 questions measuring five critical-thinking skills and compared the critical thinking ability within the Air Force to a general population.[12] His results were published in the fall of 2008 and exposed the lack of critical thinking skills within the workforce of the Air Force.[13] The 180 Air Force officers who were tested scored well below average when compared to the graduate degree norm group.

While studying at the Air War College (AWC) in 2015, Colonel Stone conducted a similar study of officers' critical thinking skills at Air Command and Staff College (ACSC), AWC, and the School of Advanced Air and Space Studies (SAASS). In this study, SAASS students scored in the 61st percentile, while ACSC and AWC students scored in the 36th percentile.[14] The 2015 study criticized the Air Force's failure to educate and train its personnel to develop adequate critical-thinking skills in professional military education programs. Despite Colonel Stone's indictments of the Air Force's demonstrated lack of critical-thinking capability and repeated call-outs from others in the workforce, there are no significant and sustained efforts to measure, develop, and assess these essential cognitive skills within the workforce.[15]

In addition, periodically measuring critical thinking alone is insufficient. For instance, one may score well on the WGCTA or some similar test indicating they possess the ability to critically think but due to time constraints and other demands and distractions, there is no guarantee that information warriors will consistently produce analytical products, provide recommendations, and make decisions that are the result of and demonstrate higher-order thinking. Since these "higher-order" thinking capabilities are central to effective information warrior activities, there is a compelling need for a systematic means to address this "higher-order" thinking skills deficit. Therefore, a need exists to not only train the Air

Force's information warriors on these skills but also to "operationalize" this capability with the assistance of technology by leveraging human-machine teaming that ensures critical and higher-order thinking is integrated into their daily work.

The above statistics and Air Force practices bring focus to the three prominent causes of why information warriors are not realizing their potential nor fully exploiting the full range of their cognitive capabilities:

- Inadequate higher-order thinking skills upon leaving formal education
- Insufficient training and assessment focused on developing higher-order thinking skills
- The lack of a structural means for supporting and enhancing higher-order thinking and associated activities while creating work products

Defining Higher-Order Thinking Skills and Processes

One can find many ways for defining and characterizing "higher-order thinking" in the published literature and this article makes use of and combines concepts expressed across several widely accepted sources. Disambiguating the various terms and describing a useful "higher-order thinking taxonomy" is the starting point.

What is "higher-order thinking?" The 1987 National Research Council report *Education and Learning to Think* provided an excellent concise summary: Higher order thinking involves a cluster of elaborative mental activities requiring nuanced judgment and analysis of complex situations according to multiple criteria. Higher order thinking is effortful and depends on self-regulation. The path of action or correct answers are not fully specified in advance. The thinker's task is to construct meaning and impose structure on situations rather than to expect to find them already apparent.[16]

While informative, concise, and potentially familiar sounding to many information warriors, this National Research Council definition is not sufficiently detailed to serve as the basis for actionable specifications of a "higher-order thinking learning or support system." As such, it is useful to further disaggregate "higher-order thinking" into more discrete skills and thinking processes that enable a more systematic actionable approach.

Higher-Order Thinking Skills

The list of discrete "higher-order thinking skills" in the table below is largely categorized as per B. S. Bloom and David R. Krathwohl.[17] It is further augmented with those higher-order skills expressed by R. H. Ennis, P. Facione, J. D. Bransford, the National Research Council, and Ross D. Arnold.[18]

Table. Higher-order thinking skills

1. Investigating and Observing Keenly	
• the situation • entirety of context • system and overarching structure • distinguishable details within the context • objects, behaviors, and forces	• elements and components • characteristics and attributes • magnitudes and measures • boundaries • statics and dynamics
2. Understanding	
• questioning • defining/clarifying • contextualizing/framing/scoping	• determining objectives • relating cause and effect • comprehending concepts, models, knowledge
3. Applying/Transferring	
• applying concepts and/or models to new circumstances • using concepts and/or models to derive insights • modifying concepts and/or models to meet new needs	• extending understandings to new contexts/situations • applying general principles to specific circumstances • applying lessons from analogous situations • testing/experimenting
4. Analyzing	
• identifying, characterizing, interpreting, organizing • defining dimensions of differentiation and homogeneity • distinguishing/differentiating • ranking/prioritizing • grouping/categorizing • comparing • quantifying/calculating • dissecting/disaggregating	• revealing individual parts and attributes • describing the context, its parts and functions • relating the full set of parts to the whole • uncovering patterns and relationships • uncovering factors that impact • uncovering issues • revealing assumptions • determining relevance & applicability • clarifying and making sense
5. Synthesizing	
• deducing • inducing • inferring/deriving • generalizing from specifics • abstracting • analogizing • connecting disparate elements into something of meaning • seeing relationships between elements • creating a concept or model • incorporating time, sequence, and dynamics	• planning • estimating/approximating • imagining/inventing • designing/creating • anticipating • theorizing • predicting • generating alternatives • hypothesizing/positing/explaining • constructing arguments/reasoning • creating meaning
6. Evaluating	
• establishing criteria • weighing/judging • criticizing • appraising/assessing • reflecting/reviewing • deciding/selecting/choosing	• recommending • supporting • concluding • uncovering biases • self-evaluating thought processes and dispositions (metacognition and self-regulation)

While this "skills" list is extensive and reflects a robust aggregation from the literature on higher-order thinking skills and processes, the list is not exhaustive. However, an "exhaustive" list is not needed here. The point of this list is to convey,

in large measure, those discrete thinking skills and abilities that (1) sufficiently indicate what is meant by higher-order thinking skills, (2) are useful for empowering individuals to succeed in those contexts that require higher-order cognitive competencies, (3) are illustrative of the discrete measurable skills that should be developed, exercised and assessed by training technologies, and (4) should be integral to any structural method for supporting and enhancing information warrior higher-order thinking while on the job.

Higher-Order Thinking Processes

There are many different contexts for applying the previously listed higher-order thinking skills, and each different context may call upon individuals to use a subset of these skills toward a desired end. As used in this paper, a higher-order thinking "process" is the application of some subset of the higher-order thinking "skills" to achieve a particular end in a given context.

Some higher-order thinking processes are broadly applicable across many disparate contexts and others are more narrowly focused on specific contexts. For example, "critical thinking," "creative problem solving," and "rational decision-making" are all higher-order thinking processes that are broadly applicable across many contexts. On the other hand, "scientific thinking," and "strategic thinking" are often referenced in slightly more "specialized" contexts. While these five examples of "higher-order thinking processes" have different names and may be applied in different contexts, they often call upon individuals to exercise very similar subsets of higher-order thinking skills from the table as there is a good deal of overlap. For example, scientists often refer to "scientific thinking" as "critical thinking" being applied to a scientific context. Business executives often describe the process of decision-making as a combination of critical thinking and creative problem-solving. So, while investigating scientific phenomena or making corporate decisions are very different contexts, those processes often share many (though not all) of the same higher-order thinking skills.

What follows are the widely cited definitions of the five aforementioned processes that are closely aligned with "higher-order thinking."

Critical thinking. "Critical thinking is reasonable reflective thinking focused on deciding what to believe or do."[19] In describing this elegant and expansive definition, Ennis also extensively details the rich set of underlying higher-order thinking skills (which he calls "abilities"), which characterize the critical thinking process. His set of "abilities" are encompassed by the higher-order thinking skills in the table. In addition to the very broad scope of higher-order thinking skills that comprise critical thinking, the wide applicability of the critical thinking process is highlighted by its defined purposes: "deciding what to believe" as well as

"deciding what to do." This wide applicability encompasses many other "higher-order thinking processes."

Creative problem solving. Creative problem solving is finding the ways for resolving the "discrepancy between an initial state and a goal state, when there is no ready-made solution."[20] It is worthy to note that "Improving Critical Thinking" is a subtitle of Bransford's 1993 book and with good reason. Identifying the "initial state," the "goal state," and deciding on "ways for resolving the discrepancy" between the two states will necessitate the use of many of the higher-order skills from the table that are shared in common with critical thinking.

Rational decision-making. Peter Drucker defines decision-making as a judgment; it is a choice between alternatives.[21] R. L. Trewatha defines decision-making with a bit more information: "Decision-making is the selection from among possible alternatives in order to arrive at a solution for a given problem."[22] In both Drucker's and Trewatha's definitions, decision-making is a particular category of problem-solving. Like problem-solving, identifying alternatives, analyzing the relevant information, and deciding the best among them will necessitate the use of many of the higher-order skills from the table. It is also interesting to note that decision-making is a fundamental element of the critical thinking definition, in other words, "reasonable reflective thinking focused on *deciding* what to believe or do." Thus, higher-order thinking skills relevant to critical thinking are similarly relevant to decision making.

Scientific thinking. Scientific thinking is the pursuit of understanding and explanations, based upon inquiry, experimenting, investigating, fact-gathering, analyzing, theorizing, modeling, hypothesizing, reasoning, evaluating, and arguing.[23] Not only are all these "thinking practices" also "higher-order thinking skills" but so too are the many thinking skills which these particular "scientific practices" encompass. For example, the term *reasoning* as a scientific practice includes deducing, inducing, deriving, inferring, generalizing, and so forth, all of which are "higher-order thinking skills" (per the table). Any survey of the literature on scientific thinking will see close alignment between the higher-order thinking skills of the table and those associated with scientific thinking. Scientific thinking is also highly consonant and consistent with critical thinking (i.e., the "reasonable reflective thinking focused on deciding what to *believe*").

Strategic thinking. Strategic thinking is the thoughtful process of configuring ends, ways, and means to achieve an objective, given a set of (often dynamic) circumstances.[24] This definition is well-aligned and consonant with the definitions of critical thinking, creative problem solving, and decision-making. As such, the higher-order thinking skills applicable to strategic thinking are the

same as those of critical thinking, problem-solving, and decision-making, albeit in a strategic context.

To summarize, "higher-order thinking skills" are those complex cognitive skills and abilities as broadly characterized by the National Research Council and as more discretely identified in the table.[25] A "higher-order thinking process" is a collection of those higher-order thinking skills that are used to achieve an end in a particular context. Helping information warriors to more fully develop and systematically employ these higher-order thinking skills and processes will greatly enhance our information warfare capabilities.

A Strategic Approach to Developing, Exercising, and Assessing Higher-Order Thinking Skills and Processes

The strategic approach entails two elements: (1) understanding the higher-order thinking skills and processes important for the information warrior, and (2) designing a scalable, automated, web-based interactive technology that enables one to efficiently learn these cognitive skills using a methodology that is aligned and consonant with widely accepted expert learning theory. The previous section provided a clear description of the higher-order thinking skills and processes that are desired and necessary. This section discusses the expert learning theory that will enable the efficient and effective learning of these essential skills.

In his widely cited work, *How People Learn*,[26] Bransford makes clear that "learning with understanding" and achieving the ability to "transfer" those understandings to different contexts is developed and enhanced by several factors, beginning with Piaget's theory that learners construct understanding by actively engaging with a domain, and, construct their conceptual scaffolding in response to their findings from the interactions.[27] That is, individuals develop understanding and their cognitive capabilities by accommodating preexisting conceptions and assimilating new learnings from active exploring and experiencing.[28] However, Bransford makes clear that having learners construct understanding completely independent of guidance can in many instances be less than optimal; that without some guidance, new constructions of understanding can potentially be misdirected. Therefore, the dual combination of constructing one's understanding through independent cognitive effort being followed-up with a dose of guidance is very powerful. As Bransford states: "usually after people have first grappled with issues on their own, "teaching by telling" can work extremely well."[29]

In addition to the important dual process of having learners independently actively construct their conceptual scaffolds in combination with assistance from expert guidance, Bransford describes other factors affecting the ability to learn

with understanding and transfer, including metacognition, time-on-task, learner motivation, context, and engaging with authentic problems.

Metacognition

Learning is enhanced when individuals take responsibility and recognize what they understand and when they need more information.[30] Metacognition refers to an individual's ability to predict their own performances and to monitor their current levels of mastery and understanding.[31] Instructional practices congruent with this approach include enabling sense-making, self-assessment, and reflection on what worked and what needs improving. These practices have been shown to increase the degree to which learners transfer their learning to new settings and events.[32]

For learners to "self-assess" and gain insight into their learning and their understanding, frequent feedback is critical. Feedback is most valuable when students can use it to revise their thinking as they are working. Responsive formative assessment increases students' learning and transfer, and they learn to value opportunities to revise.[33]

Time-On-Task

In all domains of learning, the development of expertise occurs only with major investments of time, and the amount of time it takes to learn the material is roughly proportional to the amount of material being learned.[34]

Learner Motivation

Motivation affects the time and effort that people are willing to devote to learning. Students are motivated to spend the time needed to learn complex subjects and to solve problems that they find interesting. Humans are motivated to develop competence and to solve problems; they have, as R. W. White put it, "competence motivation."[35] Although extrinsic rewards and punishments affect behavior, people work hard for intrinsic reasons, as well. Challenges, however, must be at the proper level of difficulty to be and to remain motivating; tasks that are too easy become boring; tasks that are too difficult cause frustration.

Context

Transfer is also affected by the context of original learning; people can learn in one context yet fail to transfer to other contexts. Research has indicated that transfer across contexts is especially difficult when a subject is taught only in a

single context rather than in multiple contexts.[36] The issue is how to promote a wide transfer of learning. One way to deal with a lack of flexibility is to ask learners to solve a specific case and then provide them with an additional, similar case; the goal is to help them abstract general principles that lead to more flexible transfer.[37]

Transferring Beyond the Classroom—Employing Authentic Problems

A primary goal of learning is to be able to access and apply information where it is needed, and to be able to transfer what is learned to relevant circumstances. There is much value to the idea that learning should be organized around authentic problems that are frequently encountered in non-school settings: in John Dewey's vision, "School should be less about preparation for life and more like life itself."[38] The use of problem-based learning in medical schools is an excellent example of the benefits of looking at what people need to do once they graduate and then crafting educational experiences that best prepare them for these competencies.[39] For this reason, case-based learning is often employed where relevance to the workplace is important.

A Systematic Means for Developing & Measuring Higher-Order Thinking Skills

The above theories and principles are foundational for successful learning. As such, they were incorporated as the central elements in the design of a new online platform that measures, develops, exercises and assesses higher-order thinking skills and processes. This innovative platform was created by findingQED, a company focused on providing a systematic, scalable, and effective means for significantly improving higher-order thinking capabilities.

Embodied within findingQED's unique online platform is a powerful framework that calls upon learners to investigate, analyze, and resolve issues arising in scenarios of relevance to the learner, and for learners to support their perspectives by constructing explicit well-reasoned fact-based arguments. Higher-order thinking skills are developed, exercised, and measured during the learner's interactive investigations, sense-making, fact gathering, analyzing, finding connections, applying methods and models, deriving inferences, judging and assessing, specifying perspectives, and constructing supporting arguments. Probabilities, levels of certainty, and the number of reasonable resolutions can vary from scenario to scenario as can the quantity and types of digital media to be evaluated. Importantly, instructive automated descriptive feedback is combined with detailed quantitative

measures to provide immediate rich personalized guidance that empowers each learner to reflect upon and improve their higher-order thinking.

Custom scenarios that incorporate any type of digital media (video, photos, graphics, PDFs, audio, etc.) can be efficiently created by anyone using the platform's scenario creator interface and can pertain to any context, subject matter and issues deemed relevant by the scenario creator for their particular set of learners. Having subject matter experts create scenarios on the platform with the aim of measuring, exercising, developing, and assessing analyst higher-order thinking skills as applied to resolving issues arising in situations that are directly relevant to the analysts' domain is exactly the type of use envisioned for the platform. The platform framework ensures that, regardless of the scenario context, the learner's higher-order thinking, critical thinking, and problem-solving processes are systematically developed in accord with widely accepted cognitive theories and learning principles.

In addition to developing higher-order thinking skills in a training context, the findingQED platform and framework can also provide a structural means for infusing these important cognitive abilities into the information warrior's actual operational work activities.

A Structural Means for Supporting and Enhancing Higher-Order Thinking by Information Warriors in Their Work Activities

While higher-order thinking skills development is important and necessary in any information warrior training program, it is not sufficient. A platform that supports and enhances information warrior higher-order thinking in their actual operational work activities is also necessary for ensuring greater warrior effectiveness. That is, the information warrior needs a structural method to ensure that all "relevant elements of thought and reasoning" are applied to each work assignment; in other words that the requisite higher-order thinking skills and processes are brought to bear on the warrior's information production.

There are at least six areas of strategic gains that information warriors can achieve by employing a structural means for explicitly incorporating all "relevant elements of thought and reasoning" in their process and practice. Employing such a method in their work process will:

1. Systematically enhance information warrior cognitive capabilities.
2. Foster systematic continuous learning and improvement.
3. Enable more efficient collaboration and sharing of relevant elements of thought and reasoning across organizational divisions and stovepipes.

4. Enable a network of "inter-level" interactions about relevant elements of thought and reasoning, as an overlay to the existing information-flow hierarchy.
5. Provide a flexible dynamic means for rapidly modifying any aspect of underlying thoughts and reasoning to efficiently generate alternative scenarios and test sensitivities.
6. Enable more rapid and accurate assessment and management of workforce capabilities.

Systematically Enhance Information Warrior Cognitive Capabilities

As detailed in previous sections, effective information warrior work activities depend upon a wide array of cognitive capabilities. But much of the workforce does not consistently excel across all required cognitive skills. These shortfalls can and should be structurally and systematically remedied, with the result being a more insightful, consistent, comprehensive, accurate, reliable, and efficient information product. The findingQED platform is a cost-effective developmental technology that can structurally support and empower all information warriors to enhance their cognitive capabilities during their work process. While the platform can be effectively utilized in any context requiring higher-order thinking, the authors intend to prioritize the platform's configuration and use to empower intelligence analysts to advance the conduct of information warfare. Doing so will enable the Air Force to better employ the information element of power in pursuit of national interests. It will:

- Prevent emotion from overwhelming the ability to reason
- Foster higher-order and critical thinking
- Prevent assumptions and uncertain inferences from being treated as facts
- Enable more explicit and effective assessment of probabilities
- Foster more well-reasoned fact-based logical arguments
- Ensure a science-based, data-driven-process with the understanding that science is seldom 100 percent settled
- Remain objective, adjusting conclusions based on the latest evidence and testing

Foster Systematic Continuous Learning and Improvement

Creating a culture of continuous learning and improvement is a goal for any organization. This is essential for organizations involved in areas that are strategically consequential and experiencing dynamic change, as exemplified by the information warfare arena. A culture of learning will support individuals to systematically increase their capabilities and effectiveness, which is especially necessary when change brings new opportunities and threats. Aggregating gains in learning and improvement across the organization and over time will have a profound impact on information warfare readiness and effectiveness.

Such a culture does not happen through words; it must be supported with a systematic approach, tools, and process. With the findingQED platform, individuals would not only have a tool to systematically support their thought processes in their work product creation, but such a structural interactive platform would also encourage consistent self-reflection about all their elements of thought and reasoning, and enable rapid and efficient sharing with more experienced personnel who can rapidly provide evaluation and feedback, which of course is a key element for continuous learning and improvement.

In addition to individual development, there are organization-wide gains available. One such gain is the storage of and reference to any professional's investigatory observations, understandings, analyses, interpretations, assumptions, inferences, insights, connections, relationships, evaluations, judgments, assessments, probabilities, alternative points of view, and entire reasoning chains. Having ongoing and historical access to all the relevant elements of thought and reason can be quite valuable to others in the organization.

Although there are multiple ways to incentivize regular use of the platform to improve higher-order thinking, fearless accountability for learning and improvement will most quickly instill a culture of excellence and superior performance. Having a structural capability for creating, storing and manipulating "relevant elements of thought and reasoning" is a valuable asset not only for (1) enhancing information warrior cognitive capability and work product effectiveness, (2) individual reflection, feedback and improvement and (3) use as a historical reference, but also (4) to provide input to prospective artificial intelligence system learning engines, when and where appropriate.

Enable More Efficient Collaboration and Sharing of Relevant Elements of Thought and Reasoning across Organizational Divisions and Stovepipes

Information is currently shared across organizational divisions and stovepipes where and when it is "needed." However, the "tough problems, the complex ones" often require multisource and/or specialized input that would be more useful if based on the full set of existing elements of thought and reason. Hence, it would be highly productive to have an efficient structural means to ask for and receive input from the most appropriate personnel across different organizational divisions, who can provide their analyses and perspectives based upon the full set of most current "work-in-process" elements of thought and reasoning, rather than just on the raw information or "final reviews." Such collaboration may even extend to persons providing unsolicited insights about relevant elements of thought and reasoning that they could view on the platform. The collaboration should be as broad as is permissible across the organization, subject to the necessary security constraints in certain circumstances. For tough problems, the more collaboration from invited eyes and minds on the relevant elements of thought and reasoning, the better the result is likely to be. The web-based findingQED platform can enable such efficient and effective collaboration.

Enable a Network of "Inter-Level" Interactions about Relevant Elements of Thought and Reasoning as an Overlay to the Existing Information-Flow Hierarchy

Currently, information product formulation is often the result of a hierarchical structure. That is, many information gatherers are feeding their (often highly focused) findings upward through additional levels of information filtering and aggregation, with the ultimate insight generation or point of view created by far fewer at the top of this filtering and aggregation pyramid. The question is not if this works; it has. The question is if this should be the only systematic process, exclusive to all others. Might there be other efficient and useful ways to augment this traditional process and further leverage the information warriors' capabilities?

A hierarchical information filtering and aggregation architecture most certainly does not always leverage the capabilities of the organization nor of the many highly capable warriors that exist "lower in the food chain." Certainly, less senior analysts could have an insightful impact on some issues that have already been filtered and aggregated at a higher level. But presently, not enough of this "lower-to-upper-level" iterative input is undertaken and is not sufficiently leveraging the

totality of the cognitive value of the entire workforce. As a result, the Air Force is, unnecessarily, leaving untapped information warrior value on the field.

Without disrupting the architecture of the existing hierarchical process, an efficient and impactful "network architecture approach" can be overlaid and enable efficient "inter-level" iterative interaction pertaining to the relevant to elements of thought and reasoning, and by so doing, unleash significant amounts of cognitive value into the existing processes.

If the information production process included an explicit means for creating, storing, and manipulating relevant elements of thought and reasoning, several others, regardless of level in the hierarchy could review and provide input, potentially yielding key insight value on an issue. For example, it is possible that a newly discovered or re-introduced relevant piece of information could change a point of view or reasoning chain if that piece of information was known by the decision-maker. It may be that the relevant information was filtered, or simply did not seem relevant until the aggregation process proceeded and led to a point of view. If the individual who knows this "now relevant information" is not privy to the full reasoning chain and resultant point of view, the decision-maker(s) are deprived of this potentially relevant insight. This example is just one of many scenarios where potentially useful information is not connected where and when it is needed because of the existing hierarchical process.

This flaw of process and organizational structure is avoidable. By utilizing a structured means for producing information that makes visible all the detailed relevant elements of the thought and reasoning, and by inviting those who can provide feedback and input into the process, regardless of position in the hierarchy, one can unlock useful information and increase value in the process. Would it not be useful (of course, accounting for security considerations) to have all relevant information warriors to see, reflect on, and potentially provide input on the various discrete elements of observations, understandings, analyses, interpretations, assumptions, inferences, insights, connections, relationships, evaluations, judgments, assessments, probabilities, alternative points of view, entire reasoning chains, and other relevant elements of thought and reasoning that are pertinent to an important information product and resulting consequential point of view? Does one's level in the hierarchy matter if they have a valuable contribution to make? Utilizing the findingQED platform that structures information products into highly useful and reference-able discrete "elements of thought and reasoning" could help unlock the strategic untapped value that resides within our information warriors.

Providing a Flexible Dynamic Means for Rapidly Modifying Any Element of Underlying Thought and Reasoning to Efficiently Generate Alternative Scenarios and Test Sensitivities

Often, the objective of intelligence analysis is to create a point of view that: assesses, describes, explains, predicts, prescribes alternatives, or decides. Therefore, it is often the case that there are different alternatives and differing levels of probability or uncertainty. Given this, it can be very useful to examine and vary one or more of the underlying relevant elements of thought and reasoning, including the key facts, analysis, interpretations, inferences, assessments, probabilities, and judgments to determine how possible changes in one or more of these individual elements will impact the ultimate point of view. If all the underlying thought and reasoning elements are not entirely explicit and clear, then conducting a sensitivity or alternatives analysis could be dangerously flawed. Further, if it is difficult to roll-up probabilities across all the elements of the reasoning chain, such an analysis would be cumbersome. By having a structured means for creating, storing, and manipulating all the relevant elements of thought and reasoning supporting a particular point of view, including its entire reasoning chain, conducting such a sensitivity or alternatives analysis would be efficient, thorough, and comprehensive. This will be a very powerful tool for many uncertain situations.

Enable Rapid and Accurate Assessment and Management of Workforce Capabilities

Understanding who is best able to accomplish tasks accurately and reliably is of critical importance. Understanding who has the potential to advance, and who shows continual improvement, is also of great importance. So too is understanding who is not progressing appropriately. Knowing these facts with some certainty is key to making assignments that can have serious consequences.

By having a structural method that enables one to create, store, and manipulate all the relevant elements of thought and reasoning about any analytical project provides operational and talent managers with an objective, explicit, and transparent method for evaluating and assisting personnel. Such a system enables a clear and transparent view of everyone's higher-order thinking skills and provides the robust means to support and train them where the assessment of the thought and reasoning output shows need. Viewing and assessing each person's cognitive abilities becomes transparent for managers, thus enabling specific assistance, intervention, support, advice, and training. This can be accomplished in real-time, all while information warriors are on the front line performing their tasks and responsibilities; their work activities can be reviewed at any time by their supervi-

sors. As such, the findingQED platform configured to support analytical production can be a powerful talent management tool in addition to providing training and operational support for advancing the Air Force information warfare mission.

Summary

The Air Force is significantly and systematically under-utilizing a strategic asset, the mind of the information warrior. This is a result of under-investing and not providing consistent broad-based thorough development of higher-order thinking skills in information warrior training and not providing a structured means for ensuring the systematic use of these skills in operations. These shortfalls can be remedied by incorporating systematic training methods focused on developing higher-order thinking skills as well as employing a structural means for infusing these elements of thought and reason into the operational work practices of the warriors. The findingQED company's mission is to remedy these shortfalls and has a powerful online platform that measures, develops, exercises, and assesses higher-order thinking skills using interactive scenarios that are contextually relevant to the learner. As well, the platform's framework can be deployed as a tool to infuse higher-order thinking into the information warrior's analyses and work activities.

This human-machine teaming, for enhancing both training and work processes, will empower the information warfare workforce to achieve large-scale increases in capability and effectiveness. By incorporating such structural and systematic methods, the Air Force will add a powerful strategic means for outpacing competitors in the contest for information dominance. ✪

Jay Fudemberg

Mr. Fudemberg (BS, University of Texas in Austin; MBA, Stanford University) is the founder and CEO of findingQED, a provider of digital technology that develops higher-order thinking skills and empowers individuals to think more insightfully in information-intensive environments. Among his prior senior executive roles, Mr. Fudemberg was a strategy consultant with Bain & Company, an international management consulting firm where he specialized in leveraging technology to gain competitive advantage. He was a software engineer earlier in his career.

Lt Col Robert D. Folker, Jr., USAF, Retired

Lieutenant Colonel Folker (BS, Excelsior College; MS, National Intelligence University) is the senior strategist and intelligence consultant at PatchPlus Consulting, Inc., and the former commander of the 7th Intelligence Squadron. Previously, he served as a Checkmate strategist and program element monitor on the Air Staff. Before his assignment at the Pentagon, he served as the director of operations for the 19th Weapons Squadron, US Air Force Weapons School. As an intelligence officer, he conducted sensitive reconnaissance operations across the globe and served in combat during Operations Enduring Freedom and Iraqi Freedom.

Notes

1. Lt Gen Timothy Haugh, USAF, and Lt Gen David Deptula, USAF, retired, interview with the commander, Sixteenth Air Force, AF Cyber, and Joint Force HQ-Cyber, Aerospace Nation, 15 July 2020, YouTube video, 1:16:13, https://www.youtube.com/.

2. This sentence references the Sixteenth Air Force's three lines-of-effort mentioned in the Lt Gen Timothy Haugh interview—generate insights, compete now, and manage escalation, and provides context for how the proposal in this article can help provide the convergence needed to achieve desired outcomes.

3. Donald M. Bishop, "DIME, not DiME: Time to Align the Instruments of U.S. Informational Power," *Strategy Bridge*, 2018, https://thestrategybridge.org/.

4. Steven Heffington, Adam Oler, and David Tretler, *A National Security Strategy Primer* (Washington, DC: National Defense University Press, 2019), https://nwc.ndu.edu/, 27.

5. Brandon C. Kasubaski, "Exploring the Foundation of Multi-Domain Operations," *Small Wars Journal*, 2019, https://smallwarsjournal.com/.

6. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018, https://dod.defense.gov/, 5.

7. Air Combat Command Public Affairs, "ACC Announces 24th and 25th NAF Merger," 5 April 2019, https://www.af.mil/.

8. Carmine Cicalese, "How to Give the Military's Tactical Information Warriors a Chance," F*ifth Domain*, 9 August 2019, https://www.fifthdomain.com/.

9. Robert Kozloski, "Creating Cognitive Warriors," *Naval Agility*, 3 August 2015, https://www.secnav.navy.mil/.

10. Educational Testing Service, "Summary of Proficiency Classifications, Seniors with More than 90 Hours, Four Year Colleges and Universities," 30 June 2013, ETS Proficiency Profile, Annual Comparative Data Guide.

11. American Association of Colleges and Universities, "Falling Short?" College Learning and Career Success," 15 January 2015, "AACU Report: Selected Findings from Online Surveys of Employers and College Students."

12. Goodwin Watson and Edwin Glaser delineated the five skills of critical thinking: inference, recognition of assumptions, deduction, interpretation, and evaluation of arguments.

13. Col Adam J. Stone, "Critical Thinking Skills of Air Force Intelligence Officers: Are We Developing Better Critical Thinkers?," master's thesis, 2008, National Defense Intelligence College.

14. Col Adam J. Stone, *Critical Thinking Skills of US Air Force Senior and Intermediate Developmental Education Students* (Maxwell AFB, AL: Air War College, 2016).

15. Lt Col James D. Davitch, USAF, and Lt Col Robert D. Folker, Jr., USAF, "Operationalizing Air Force Critical Thinking," *Air and Space Power Journal 31, no. 4,* 62–67, https://www.airuniversity.af.edu/.

16. National Research Council of the National Academies, *Education and Learning to Think* (Washington, DC: National Academies Press, 1987), https://doi.org/.

17. B. S. Bloom et al., "Taxonomy of Educational Objectives: The Classification of Educational Goals," Handbook I: Cognitive Domain (New York: David McKay Company, 1956); and David R. Krathwohl, "A Revision of Bloom's Taxonomy: An Overview," 2002, *Theory Into Practice* 41, no. 4, https://www.depauw.edu/.

18. R. H. Ennis, "Critical Thinking: Reflection and Perspective—Part I," *Inquiry: Critical Thinking Across the Disciplines* 26, no. 1 (2011): 4–18, https://philpapers.org/; and P. Facione,

"Critical Thinking: What It Is and Why It Counts," 1 January 2015, Insight Assessment; and J. D. Bransford, A. L. Brown, and R. R. Cocking, *How People Learn: Brain, Mind, Experience, and School* (Washington DC: National Academy Press, 2004); J. D. Bransford and B. S. Stein, *The Ideal Problem Solver (*New York: Worth Publishers, 1993): National Research Council of the National Academies, *A Framework for K-12 Science Education: Practices, Crosscutting Concepts, and Core Ideas*, (Washington DC: National Academies Press, 2012): 41–82; and Ross D. Arnold and Jon P. Wade, "A Definition of Systems Thinking: A Systems Approach," *Procedia Computer Science* 44 (2015): 669–78, https://www.sciencedirect.com/.

19. Ennis, "Critical Thinking: Reflection and Perspective," 4-18.

20. Bransford and Stein, *The Ideal Problem Solver*, 1-–130.

21. Peter Drucker, *Management: Tasks, Responsibilities, Practices* (New York: Harper & Row, 1973), 465–80.

22. R. L. Trewartha and M. G. Newport, *Management, 3rd Edition* (Dallas: Business Publication Inc., 1982), 145–48.

23. National Research Council, *A Framework for K-12 Science Education,* 41–82.

24. Lawrence Freedman, *Strategy, A History* (Oxford: Oxford University Press, 2013).

25. National Research Council, *Education and Learning to Think,* 1–48.

26. J. D. Bransford, A. L. Brown, and R. R. Cocking, *How People Learn: Brain, Mind, Experience, and School* (Washington DC: National Academies Press, 2004).

27. Bransford, Brown, and Cocking, *How People Learn*, 1–113.

28. P. Cobb, "Theories of Mathematical Learning and Constructivism: A Personal View. Symposium on Trends and Perspectives in Mathematics Education," 1994, conference conducted at the meeting of the Institute for Mathematics, University of Klagenfurt, Austria; Jean Piaget, *The Origins of Intelligence in Children*, M. Cook, trans. (New York: International Universities Press, 1952); Piaget, *The Child and Reality: Problems of Genetic Psychology* (New York: Penguin Books, 1973; Piaget, *The Language and Thought of the Child* (London: Routledge and Kegan Paul, 1973); Piaget, *The Grasp of Consciousness* (London: Routledge and Kegan Paul, 1977); Piaget, *Success and Understanding* (Cambridge, MA: Harvard University Press, 1978); L. S. Vygotsky, *Thought and Language* (Cambridge, MA: MIT Press, 1962); and Vygotsky, *Mind in Society* (Cambridge: Harvard University Press, 1978).

29. D. L. Schwartz and J. D. Bransford, "A Time for Telling," *1998, Cognition and Instruction* 16, no. (4), (1998): 475-522.

30. Bransford, Brown, and Cocking, *How People Learn*, 1–113.

31. A. L. Brown, "The Development of Memory: Knowing, Knowing about Knowing, and Knowing How to Know," 1975, *Advances in Child Development and Behavior 10*, H. W. Reese, ed. (New York: Academic Press, 1975); and J. H. Flavell, "Metacognitive Aspects of Problem-Solving," *The Nature of Intelligence*, L. B. Resnick, ed. (Hillsdale, NJ: Erlbaum, 1973).

32. A. S. Palincsar and A. L. Brown, "Reciprocal Teaching of Comprehension Monitoring Activities," *Cognition and Instruction 1* (1984): 117–175; M. Scardamalia, C. Bereiter, and R Steinbach, "Teachability of Reflective Processes in Written Composition," *Cognitive Science 8* (1984): 173–190; A. H. Schoenfeld, "Problem Solving in the Mathematics Curriculum: A Report, Recommendation and Annotated Bibliography," *Mathematical Association of America Notes, No. 1, 1983*; Schoenfeld, *Mathematical Problem Solving* (Orlando, FL: Academic Press, 1985); Schoenfeld, "On Mathematics as Sense-Making: An Informal Attack on the Unfortunate Divorce of

Formal and Informal Mathematics," *Informal Reasoning and Education, 1994*, and J. F. Voss, D. N. Perkins, and J. W. Segal, eds. (Hillsdale, NJ: Erlbaum), 31–343.

33. B. J. Barron et al., "Doing with Understanding: Lessons from Research on Problem and Project-Based Learning," *Journal of Learning Sciences 7*, 1998, 271–312; P. Black and D. William, "Assessment and Classroom Learning," 1998, *Assessment and Education*, Special issue of Assessment in Education: Principles, policy and practice 5, no. 1, Carfax Pub. Co, 7-75; and N. J. Vye et al., "SMART Environments that Support Monitoring, Reflection, and Revision," *Metacognition in Educational Theory and Practice*, D. Hacker, J. Dunlosky, and A. Graesser, eds. (Mahwah, NJ: Erlbaum, 1998).

34. John Robert Anderson and Mark K. Singley, *The Transfer of Cognitive Skill* (Cambridge, MA: Harvard University Press, 1989).

35. R. W. White, "Motivation Reconsidered: The Concept of Competence," *Psychological Review 66* (1959): 297–333, https://psycnet.apa.org/.

36. Robert A. Bjork and Alan Richardson-Klavan, "On the Puzzling Relationship between Environment Context and Human Memory," C. Izawa, ed., Tulane Flowerree Symposium on Cognition, *Current Issues in Cognitive Processes* (Hillsdale, NJ: Erlbaum, 1989).

37. M. L. Gick and K. J. Holyoak, "Schema Induction and Analogical Transfer," *Cognitive Psychology 15*, 1983, 1–38, https://deepblue.lib.umich.edu/.

38. John Dewey, "My Pedagogic Creed," *School Journal 54*, no. 3, 16 January 1897, 77–80, https://infed.org/.

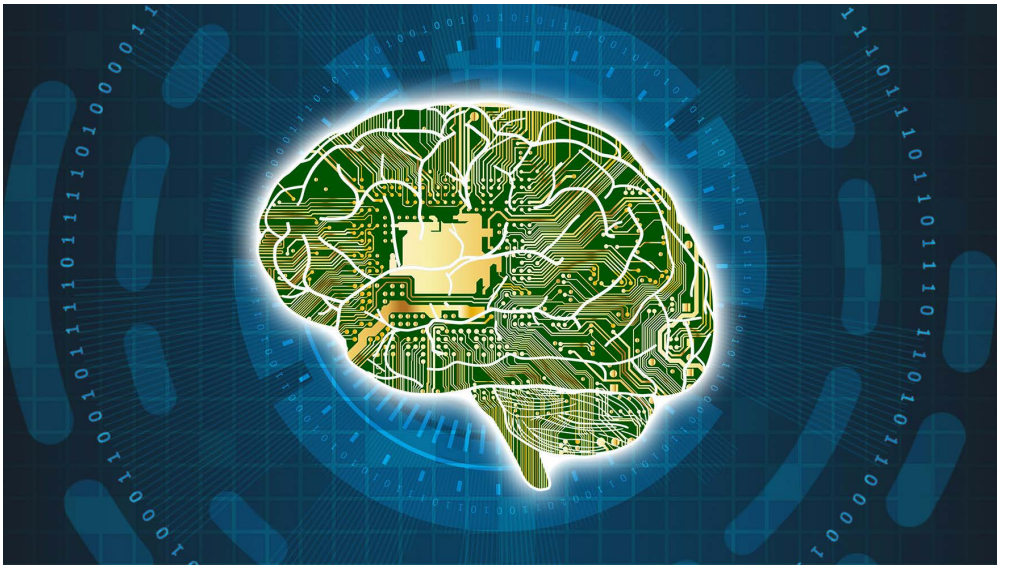
39. H. S. Barrows, *How to Design a Problem-Based Curriculum for the Preclinical Years* (New York: Springer, 1985).

FEATURE

Not All Wars Are Violent

Identifying Faulty Assumptions for the Information War

Capt Jayson Warren, USAF



"Human cognition and behavior are powerfully influenced by sets of beliefs and assumptions about life and reality."[1] When the beliefs and assumptions (inputs) are valid, the resulting actions (outputs) are also. However, when the beliefs and assumptions do not withstand scrutiny, the actions necessarily follow. The military is not immune to this phenomenon, thus, this article intends to shake the rational and emotional foundations of experientially-derived knowledge (*a posteriori*) and knowledge presumed to be self-evident (*a priori*) to remove intellectual roadblocks impeding the advancement of information warfare (IW) within the Department of Defense (DOD) and USAF. More specifically, this article analyzes the origin and implications of the following interdependent faulty assumptions that restrict the institutional thinking of Airmen: 1) All wars are violent; 2) deterrence is working if there is no violence; and 3) information warfare Airmen are *support* professionals because they do not engage in violence.

Faulty Assumption No. 1: All Wars Are Violent

Origin

Clausewitz argues war "is an act of violence to compel our opponent to fulfil our will," thereby making a distinction between an immutable nature of war and

the ever-evolving character of war where "violence arms itself with the inventions of Art and Science in order to contend against violence."[2] The key premise being, even though war is "a continuation of policy by other means," war is inherently violent and if there is no violence then a state of war does not exist. On the other hand, Sun Tzu's Eastern viewpoint contends that those most skilled in the art of war are those who win without fighting ("hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting").[3] Of these two schools of thought, the Clausewitzian framework has underpinned much of the Western world's thinking about war and peace for centuries.

Reality

Albeit two mutually exclusive definitions of war, it is important to note that validating one over the other is unproductive because they are intrinsically subjective. Instead, it must be realized that in a battle of wills, it is possible for both understandings of war to simultaneously influence its respective subscriber to act in a certain manner—which means determining the existence of a state of war lies less in whether the US believes it is physically under attack and more in whether or not adversaries are deliberately assaulting America or its national interests.

For millennia, wars were fought over existential survival, resources or treasure, and territory (or as Thucydides referred to them: fear, honor, and interest)—physical motivators that had to be seized or retained by force. However, globalization, information technologies, digital currencies, and so forth, have ushered in the ability to fight for the aforementioned without using violence or even challenging another nation's physical sovereignty. In other words, IW capabilities have blurred the lines between peace and war to the point of indistinction. In light of this, the defense community must account for the possibility that these advancements exceed anything Clausewitz could have fathomed and, as a result, the nature of war may need to include acts that are not violent. Consider the following through the perspective of existential survival, resources or treasure, and territory.

Russia. Ideas of "hybrid warfare" and "a new way of war" sprung to the forefront of the global stage after Moscow utilized the Sochi Olympics and "little green men" to obfuscate its annexation of eastern Ukraine and Crimea. However, many analysts fail to realize that most of these "publicized notions—the blurring of war and peace, that Russia is in an information war, that information can be a weapon, that nonmilitary means can be as effective as nuclear weapons—have been a part of the Russian military-theoretical debate long before the invasion."[4] Even now, and unbeknownst to many, Russia has reached beyond its *near abroad* to the point of fielding military forces worldwide that are not subject to the Ge-

neva Convention. The 2018 firefight between US and pro-Regime forces at Deir al-Zour, Syria (a.k.a. The Battle of the DAZ) brought this to light but today it extends beyond areas considered war zones. Secretly overseen by the GRU (the armed forces main intelligence directorate),[5] the Vagner (alternate: Wagner) Paramilitary Corporation (PMC) controlled by Russian oligarch and Putin-associate Yevgeny Prigozhin not only props up Moscow-friendly regimes in locales such as Syria, Libya, and Venezuela,[6] it also interferes in the sovereign affairs of nations rich in natural resources (e.g., gold, uranium, diamonds) to facilitate beneficial conditions for Russian companies (e.g., Sudan, Central African Republic).[7] Vagner functions as an undeclared branch of Russia's armed forces (e.g., transported on Russian military aircraft, treated in Russian military hospitals, operate jointly with Russian military forces, and receive Russian medals signed by Putin),[8] thereby providing plausible deniability. This plausible deniability is subsequently "leveraged by the Kremlin in its military strategy to stall adversaries' responses and make short-term strategic gains."[9]

China. While by no means defending their atrocious human rights record, the Chinese Communist Party (CCP) is a perfect case study for the use of information (at home and abroad) to advance its own survival, resources or treasure, and territory. Despite the governmental failings of the Great Leap Forward and, more recently, the oppression that produced Tiananmen Square, the CCP engineered a population willing to fight against the US and its allies by conducting an "ideological reeducation of the public which relentlessly portrays China as the victim of foreign imperialist bullying during 'one hundred years of humiliation.'"[10] Resolving to never be humiliated again, in 2003 the CCP announced *san zhong zhanfa* (Three Warfares): 1) Strategic Psychological Operations (i.e., pre-conflict posturing of all instruments of power to intimidate and steer adversaries towards desired outcomes); 2) Overt and Covert Media Manipulations; and 3) Exploitation of National and International Legal Systems.[11] Over the next 17 years, the CCP successfully annexed the South China Sea; utilized its Belt and Road Initiative (BRI; a.k.a New Silk Road) as a potential worldwide Trojan horse to preposition assets, access, and resources;[12] and became the worldwide leader in intellectual property theft with estimates projecting losses up to $600 billion annually[13]—all without firing a shot.

North Korea. DPRK's cult of personality and brainwashed population is inextricably tied to the regime's pursuit of existential survival. When one examines DPRK propaganda, there is a notable aversion to intellectual discipline; "North Koreans are so much more inclined than South Koreans to settle differences of opinions with fisticuffs . . . where Stalinism put the intellect over the instincts, North Korean culture does the opposite."[14] Nevertheless, Pyongyang allowed its

understanding of violence ("fisticuffs") to evolve and presently wields robust IW capabilities despite the sanction-induced resource constraints plaguing the state. Regarding the 2014 James Franco and Seth Rogan movie *The Interview* as an attack on the regime, North Korea unleased an attack on Sony Pictures (and by extension, free speech) that cost the company millions and terrorized executives into cancelling the theatrical release. Although the Sony attack was quickly attributed to DPRK, garnering substantially less attention were the 2016 theft of $81M from Bangladesh Bank; the 2017 WannaCry 2.0 global ransomware attack; and, as reported by criminal charges unsealed in 2018, "numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities."[15] This deliberate onboarding of IW-related capabilities "is an attempt to explore the idea of asymmetric negation, probing any vulnerabilities of the US-ROK alliance."[16]

Iran. After the *Holy Defense* or the Iran-Iraq War (1980-1988), the Iranian regime believed itself to be under the residual and existential threat of Western influence. Dubbing it *jang-e narm* (soft war) in the late 2000s, the Ayatollah and Iranian conservatives view it as a strategic imperative to defend against Western culture and ideals—an obstacle to exporting the revolution and "anathema for a regime founded on Islamic values and anti-Americanism."[17] While some suggest the language is adapted from Joseph Nye's notion of "soft power" (i.e., getting another actor to acquiesce through attraction as opposed to coercion),[18] Tehran takes this a step further by not only relying on its revolutionary ideology and Persian imperial legacy (attraction) but also seeking "to influence populations and governments through manipulation and even disinformation[19] (coercion). These initiatives are symbiotically aligned with their exploitation of plausible deniability via proxies (e.g., Hezbollah, Houthis rebels, etc.) and repeated cyber assaults on global industrial and oil manufacturers.[20]

VEO. The low-cost of admission to the information environment even provides VEOs an alternative means to compete for global legitimacy—and no organization has taken this opportunity farther than the Islamic State (ISIS). Analysis of ISIS's *Twitter* and *YouTube* data revealed "linguistically diverse narratives" that spread throughout the world and remained "on message" (i.e., synchronization or what tacticians refer to as command and control).[21] ISIS also produced the online magazine *Dabiq*, combining its radical ideals with print-style media in multiple languages (Note: While *Dabiq* attained more notoriety, Islamist magazines can be dated back to 2003 with al-Qaeda's *Sawt al-Jihad* or Voice of Jihad).[22] Known as the "Digital Caliphate," ISIS's internet presence (e.g., propaganda, recruitment, battlefield videos) led some to assert the group's "vision of a global caliphate has

less to do with their desire to create a Westphalian style socio-political organization and more to do with creating a community of like-minded individuals."[23]

Clausewitz's distinction between political and military objectives is blurred when dealing with authoritarian regimes that unilaterally control all facets of governmental activities at home and abroad. Thus, when America's institutional inertia places it on a reactive footing relative to its adversaries in the information environment, strategists need to ask the right questions. For instance, asking *Was that an act of war?* would be an overgeneralization that does not account for a possible change in the nature of war (or account for whether or not adversaries believe they are waging war against the US). If Russian operatives physically stormed polling stations in 2016 or North Korean soldiers physically attacked the Sony Pictures' headquarters, the existence of a state of war would be axiomatic. But the 2+3's use of the information environment to attain the spoils of war without violence means the better question is *What is an appropriate response and how can safeguards be established to avoid such a disadvantageous situation in the future?*

Consequence of the Assumption

Despite actively holding them at risk through strategic and nuclear weaponry, post-Soviet adversaries are nevertheless deliberately countering US interests below the threshold of armed conflict. The pragmatic reality of these ever-evolving circumstances demand that war fighters re-evaluate their presuppositions about warfare and its defining traits as they seek to answer the *National Defense Strategy*'s call to great-power competition. Fixating upon violence and maintaining a bias toward conflict jeopardizes resource allocation and fosters unfounded confidence that America is the unchallenged superpower—nowhere does this manifest itself more clearly than deterrence forums.

Faulty Assumption No. 2: Deterrence is Working If There is No Violence

Origin

This assumption is deeply ingrained in military psyches and its origin is twofold: there is the conceptual understanding of deterrence as an extension of Clausewitz and there is the historical record that is interpreted as supporting evidence. These are most effectively dissected sequentially.

In terms of a Joint definition, deterrence is "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[24] However, the military's cultural bias toward conflict often reduces deterrence to holding hard targets at risk (e.g.,

nuclear weapons, bomber task force deployments) for the purpose of preempting war as defined by armed violence (Faulty Assumption No. 1). Such a context in its simplest form causes deterrence operations (i.e., "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against US vital interests"[25]) to be assessed via syllogism (if A then B; not B, therefore not A). In other words: If deterrence fails, then war will occur; war is not occurring, therefore, deterrence is not failing.

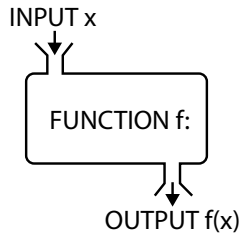
Consequently, the traditional understanding of deterrence can be conceptually explained as a mathematical function (see table 1).

Table 1. Deterrence formula

$f(x) = y$

- f = Deterrence Methods
- x = No War Desired
- y = No War Occurring

f(No War Desired) = No War Occurring



But what must be acknowledged regarding this equation is the different cognitive understanding between *Red* and *Blue* actors as to what constitutes a war (Faulty Assumption No. 1). . . to the point those evaluating the effectiveness of deterrence can theoretically mistake the following for a valid solution to the equation:

$$f(\text{No War Desired}) = \text{No "War" Occurring}$$

Nevertheless, this linear understanding of deterrence is reinforced by experientially derived knowledge from history.

America's most influential deterrence methodologies have consistently been built relative to the global context and the character of war (i.e., technological advancements) rather than an immutable nature of war. More specifically, these approaches have been rooted almost exclusively in military power and a bipolar global context. The Monroe Doctrine and Manifest Destiny was America versus European interference in the Western Hemisphere,[26] leveraging hemispheric neutrality as enabled by the Pacific and Atlantic oceans and the French and British empires underwriting international security in the global commons.

In 1945, the global context changed when the world transitioned to a nation-state bipolar construct with the US leading the free world against the USSR and the character of war changed with nuclear technology. Based on this new paradigm, deterrence was quantified in terms of preventing war between the US and

the Soviets through the concept of mutually assured destruction (or in the words of Winston Churchill, it was a time when "safety will be the sturdy child of terror, and survival the twin brother of annihilation").[27] Seeking to maintain its strategic advantage, American deterrence took the form of offset strategies—the First Offset pursued a nuclear buildup as a force-multiplier against the Soviet's numerically superior conventional forces; the Second Offset sought to use emerging technologies (e.g., stealth, precision-guided munitions) as a force multiplier against the numerical superiority of the Warsaw Pact after Moscow achieved nuclear parity. In either case, the bedrock of Cold War deterrence theory was military superiority and atomic weaponry.

In 1991, the global context changed overnight when the USSR vanished from the geopolitical stage, leaving in its place a unipolar world that would eventually become multipolar. However, the character of war slowly evolved to asymmetric (rather than an instantaneous shift as it did with Hiroshima and Nagasaki) while adversaries sought alternatives to combat the US as the remaining superpower. In the absence of one specific adversary or one specific characteristic of war to emphasize, the Cold War deterrence apparatus struggled to assimilate with a reemergent balance-of-power environment. Amidst the Kuwait invasion, President George H. W. Bush proposed multilateral cooperation as an alternative to deterrence in his 1991 State of the Union:

> What is at stake is more than one small country, it is a big idea – a new world order where diverse nations are drawn together in common cause to achieve the universal aspirations of mankind: peace and security, freedom and the rule of law. Such is a world worthy of our struggle, and worthy of our children's future.[28]

But such a collective security environment never materialized. Further complicating attempts to facilitate peace were the quantum leaps in the global context during the first two decades of the post-Soviet era—namely globalization, telecommunications technology, the opening of space as both a global commons and war-fighting domain, and the validation of nonstate actors as wartime adversaries following 9/11. As America directed its whole-of-government efforts to counterterrorism and US Central Command, the world became increasingly multipolar as nations expanded their activities in the shadows of America's gaze.

Reality

Understanding deterrence in the syllogistic form outlined above requires accepting logical fallacies. The assertion is incapable of withstanding scrutiny once the multi-faceted nature of deterrence is acknowledged—particularly because it either succumbs to circular reasoning and begging the question (How do you

know deterrence is working? Because it is obviously not failing!) or ineffectually assimilates with the burden of proof methodology in Aristotle's Principle of Non-Contradiction on the basis that the examiner must deduce that every antecedent policy was the root cause in preventing war, which would yield an infinite regression.[29] A more nuanced understanding of deterrence across all four instruments of national power (DIME) yields a more accurate picture of the geopolitical landscape, particularly in a time defined by great-power competition where actors can attain the spoils of war without armed violence.

After all, if deterrence is "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits,"[30] and adversary actions are occurring, then by definition deterrence is not only failing but has failed in the past-tense. While it is true there has not been a world war since 1945, unilaterally attributing it to deterrence would be an oversimplification. Nevertheless, there are those who argue deterrence singlehandedly prevented World War III while those on the other side contend deterrence is discredited in its entirety[31]—both are wrong, and the truth lies in the middle (e.g., deterrence did not prevent the Korean or Vietnam Wars; however, the brinksmanship during the Cuban Missile Crisis may have saved the world as it is known today). Assessing the effectiveness of deterrence operations is contingent upon one critical assumption: That deterrence is in fact working. At the risk of being anticlimactic, one cannot actually know deterrence is failing until after deterrence has failed which means the DOD must shift its understanding of deterrence away from preventing acts of violence and toward holistically preventing actions that run contrary to US interests—regardless of the mechanism an adversary employs.

As the US synchronizes its instruments of national power, the weights of effort should be allocated based on their pragmatic potential until the overarching great power competition overhaul is scoped and scaled across the whole of government. Consider the following quantified potential energies against the 2+3 (see Table 2):

Table 2. DIME potential energies against the 2+3

	Diplomatic	*Informational*	*Military*	*Economic*
Russia	Viable	Viable	Viable	Mixed Results
				Sanctions have demonstrated mixed results across conflict continuum
China	Viable	Viable	Viable	Mixed Results
				Sanctions and tariffs ongoing while US economy dependent on PRC labor/loans
North Korea	Unviable	Viable	Mixed Results	Unviable
	No diplomatic relations		Military superiority has prevented some but not all belligerency	Sanctions have crippled economy but not prevented belligerency
Iran	Unviable	Viable	Mixed Results	Unviable
	No diplomatic relations		Military superiority has prevented some but not all belligerency	Sanctions have crippled economy but not prevented belligerency
Violent Extremist Organizations	Unviable	Viable	Unviable	Unviable
	No diplomatic relations		Overwhelming military supremacy has not prevented belligerency	Informal economy; ops against revenue (oil, opioids, etc.) is military power

Information is the only instrument of national power the US currently possesses that bears potential to universally influence the behavior of the 2+3. To be clear, this is not to be misconstrued as advocating for a complete abandonment of military-led deterrence—quite the opposite, the essence of informational power relative to the character and nature of war is a foundation that requires shaking. Diplomatic power is shepherded by the Department of State, military power by the Department of Defense, and economic power by the Department of the Treasury, but informational power is not monolithic or attributable to any one agency. Since the 2017 update to Joint Publication 1: *Doctrine for the Armed Forces of the United States* established Information as the seventh joint function,[32] it is officially accepted that the DOD must lead in the information environment, but with that comes a cultural overhaul that must reconcile nonviolent power with its understanding of war's nature.

Consequence of the Assumption

Effective great-power competition is contingent upon understanding adversary intentions rather than fixating on their use of violence. For instance, when adversaries such as Russia leverage the information environment to shift their focus to

the "political goal of war rather than its means (the armed violence)," there emerges both a cognitive dissonance and a risk of unconscious/unintentional escalation when the West takes actions it perceives as being short of war (e.g., demarches, sanctions) but are understood by adversaries as being tantamount to war.[33] Competition without context is a fool's errand that inevitably devolves into jousting with windmills or self-destructive pursuits of white whales (i.e., judgment-impairing infatuations)—case in point, the misinterpretation of historical and current circumstances on the part of those still clinging to Cold War mindsets:

> And that's why we're exploring the third offset strategy. It is combinations of technology, operational concepts, and organizational constructs – different ways of organizing our forces, to maintain our ability to project combat power into any area at the time and place of our own choosing. And I want to again emphasize that the third offset is about preserving the peace, not fighting wars. And the best we believe to preserve the peace is to have a very strong conventional deterrent to convince any nation that turning to the force of arms to achieve their objectives is folly.[34]

Any attempt to deter all adversaries simultaneously would be a monumental point of departure from the Offset Strategy system. The semantic inference of the term *offset* is inherently binary—one force counteracting another. Whereas the First and Second Offsets deliberately targeted the calculus of the USSR, the so-called "Third" Offset (despite its numerical designation) would actually be a first-of-its-kind, multinodal deterrence paradigm that transcends worldview, culture, ideology, and so forth, to pierce the cognitive space of Moscow, Beijing, Pyongyang, Tehran, and terrorists concurrently.

Although deterrence is a timeless concept in both Western and Eastern theories of war, the DOD's deterrence worldview is fundamentally derived from the Cold War experience. The global context, the character of war, and perhaps even the nature of war today demand a shift in perspective. A deterrence strategy a la the proposed Third Offset proves elusive and enigmatic for two key reasons: 1) influencing the way an adversary behaves requires tailoring to how the adversary thinks (i.e., the offset strategy construct is a Cold War legacy irreconcilable with the 2+3 global context); 2) China and Russia took copious notes during the 1991 Gulf War and have spent three decades of research and development ensuring they are never rapidly dismantled in the same manner.[35] Ultimately, today's circumstances yield an environment where unilateral military advantage is not synonymous with unilateral strategic advantage—as such, because the 2+3 are severely outpacing the US in the information environment America must acknowledge that it cannot deter until it relearns to compete. For each of the individual services, relearning how to compete requires broadening the aperture of what they consider operational career fields.

Faulty Assumption No. 3: Information Warfare Airmen Are Support Professionals Because They Do Not Engage in Violence

Origin

George H. W. Bush's "new world order" never materialized and efforts toward that end were eclipsed by (to name a few) the Iraq Wars, the Balkans, Libya, and, above all, the Global War on Terror. Yet what must be realized is that all of these conflicts had a common denominator—militarily inferior opponents. In the Cold War era the military training standard was the Soviets, the deterrence target was the Soviets, and the cultural pariahs were those expressing sympathy toward the Soviets or Communism—the Cold War stance against the Soviets was not only whole-of-government but was whole-of-society; the very embodiment of Huntington's assertion "we know who we are only when we know who we are not and often only when we know whom we are against."[36] Almost 30 years of combat in the desert, predominantly against enemies declared hostile by their tactics (i.e., terrorism) rather than national affiliation, caused war-fighting skillsets to atrophy as the notion of a peer adversary fell out of vogue amidst toppling dictators and facilitating a day of reckoning for 9/11 conspirators. Thus, the *National Defense Strategy* mandate that "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security"[37] is battling the generational entropy stemming from a constituency trying to compete despite having no experience from which to know how.

For the USAF, the widespread misunderstanding of competition manifests itself in Faulty Assumption No. 3 due to its bias toward aircraft. To put this in perspective, one needs to recognize the unique approach to manpower the USAF employs vis-à-vis its sister services—the USAF is the only service that (generally speaking) sends its officers into combat while its enlisted stay behind. The Air Force's principal line-of-effort regarding manpower is its rated officer corps of pilots, navigators, and air battle managers (and by extension, its career enlisted aviators). Culturally, this line-of-effort fosters and normalizes the USAF's bias toward conflict by creating a false dichotomy between those onboard an aircraft (operations) and everyone else (support).

Reality

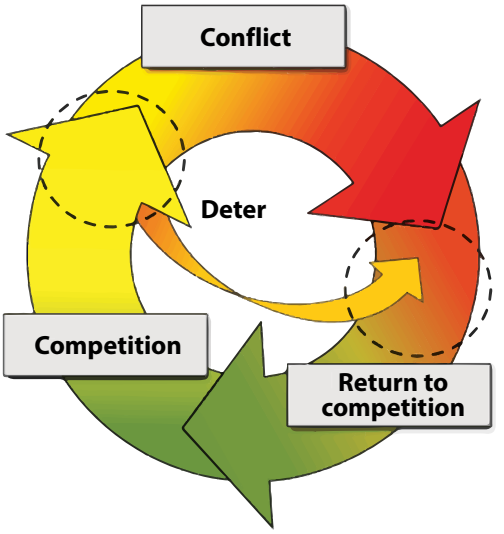
Although this anachronistic way of thinking made sense with regards to an air component's doctrinal role, the aperture for airpower in conflict and competition must be broadened if multidomain lethality is to be achieved. "Air dominance is not an American birthright. Without the U.S. Air Force's unprecedented control

of the air and enabling domains, no other U.S. military mission enjoys full freedom of maneuver."[38] As Sixteenth Air Force (AF) seeks to generate IW outcomes by expanding the weapons engagement zone of air, space, and cyber power, there is a requisite paradigm shift that needs to take place within the service—specifically reconciling the reality that professionals within the USAF's core IW capabilities (cyberspace operations; electromagnetic warfare; information operations; weather; and intelligence, surveillance, and reconnaissance [ISR]) do not provide support to war fighters but rather are themselves war fighters in the purest sense.

Moreover, IW professionals are the primary mechanism by which the USAF engages in strategic competition—far more time is spent in the competition phase than the conflict phase, thus, resources and organizational structures need to take this reality into account:

> The continuum of conflict must be understood in the current and future context. There is and always will be strategic competition. You are either winning or losing, present tense. Seldom will conflict result in a permanent win or loss. The linear depiction of peace to war and back again must be revised to reflect the cyclical nature of war where there are only positions of relative advantage (see the figure).[39]

Figure. The continuum of conflict



This is precisely why the Sixteenth AF was established.

Lt Gen Tim Haugh, Sixteenth AF commander, stated at the Sixteenth AF activation ceremony: "Our adversaries will no longer have plausible deniability. We will expose their actions that undermine international norms and take the conflict in the information environment back to them."[40] Whether its defending the USAFs vari-

ous networks; conducting cyberspace operations for US Cyber Command, US European Command, US Transportation Command, US Strategic Command, and US Space Command; executing ISR missions for every geographic combatant command; operating the signals intelligence portfolio as the service cryptologic component to the National Security Agency; or generating insights and data to produce public disclosures of adversary activities (e.g., US Africa Command's disclosure of Vagner activities in Libya),[41] Sixteenth AF is deployed in place and engaging the enemy on the front lines of the information environment daily.

Consequence of the Assumption

What must be realized is the whole-of-government is retroactively trying to establish strategy and mitigate damage from previous shortsightedness (e.g., as of 2013 the Joint Staff had banished information warfare "from its official lexicon and largely relegated information operations to a combat support role that exploits cyber tools to influence enemy cognition and decision-making processes,"[42] yet now information is a joint function and Sixteenth AF is an entire numbered air force dedicated to IW). Holding targets at risk at a time and place of its choosing has underpinned Air Force culture since 1947 (e.g., air interdiction, rapid global mobility, space and missile operations). Nevertheless, despite the ability to hit any target, any place, at any time—adversaries are still countering US interests and as such the Secretary of the Air Force directed the stand-up of a component numbered air force to bring multidomain solutions to bear on the nation's hardest problems. Unfortunately, when the stand-up of Sixteenth AF is misrepresented as an administrative "merger"[43] of Twenty-Fourth AF and Twenty-Fifth AF, rather than the construction of a brand-new war-fighting organization specifically tailored to generate IW outcomes across the continuum of conflict, then the bias towards IW as a supporting function unnecessarily restricts options available to the Joint Force—solely due to a lack of imagination and the continued acceptance of faulty assumptions.

The Way Forward

Simply put, information's efficacy as an instrument of power is understood by the 2+3 and as such they are circumventing military power by attaining the spoils of war (existential survival, resources or treasure, and territory) without engaging in a violent conflict (i.e., Clausewitz's "nature of war"). In short, their activities in the information environment is what enables the seemingly valid solution to the equation:

$$f(\text{No War Desired}) = \text{No "War" Occurring}$$

As a result, regardless of whether military strategists explicitly recognize a change in the nature of war or merely expand what they consider *violent* (Faulty Assumption No. 1), it is paramount that deterrence not be deemed *successful* solely based on the absence of force-on-force (Faulty Assumption No. 2). It is also paramount that IW professionals embrace their role as war fighters and culturally rebrand away from the false dichotomy of aviators and support (Faulty Assumption No. 3).

Within the DIME model, the only instrument with universal potential to compel global actors and encourage responsible statesmanship through accountability is information. A shift in operational plan and strategy development mindsets must account for this reality. Competition based on current methodologies and conceptual thinking possess elements of logical fallacies on the basis that the absence of *war* as Western audiences define it is not the absence of *war* as 2+3 adversaries define it—they are making gains in fear, honor, and interest without engaging in armed violence. Until the strategic initiative is regained (which it will be), IW professionals must embrace their responsibilities as members of the greater war-fighting apparatus and endeavor to eliminate plausible deniability by taking the fight back to the enemy. In the same way Winston Churchill declared "we shall fight on the beaches, we shall fight on the landing grounds, we shall fight in the fields and in the streets, we shall fight in the hills; we shall never surrender,"[44] the US must resiliently bounce back from the loss of terrain in the information environment, adapt new ways of thinking and employing the instruments of national power, and hold the line—physical or otherwise. ✪

Capt Jayson Warren, USAF

Captain Warren (AFROTC; MA, Liberty University; Graduate, USMC Weapons School) is deputy director of the Commander's Action Group, Headquarters 16th Air Force, San Antonio, Texas. He's an intelligence officer with combat search and rescue experience in Afghanistan during Operation Enduring Freedom and combat sorties as an E-8C evaluator airborne intelligence officer in Operation Inherent Resolve and Operation Freedom's Sentinel.

Notes

1. Mark E. Koltko-Rivera, "The Psychology of Worldviews," *Review of General Psychology* 8, no. 1, 1 March 2004, http://dx.doi.org/.
2. Carl von Clausewitz, *On War*, trans. J.J. Graham, 1873, accessed 26 March 2020, https://www.clausewitz.com/.
3. Sun Tzu, *The Art of War*, Allandale Online Publishing, trans. Lionel Giles, 2000, accessed 26 March 2020, https://sites.ualberta.ca/, 8.
4. Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace*, *Georgetown University Press*, 1 November 2019, 7.
5. Laurence Peter, "Syria War: Who Are Russia's Shadowy Wagner Mercenaries?" *BBC*, 23 February 2018, https://www.bbc.com/.

6. Maria Tsvetkova and Anton Zverev, "Exclusive: Kremlin-linked Contractors Help Guard Venezuela's Maduro–Sources," *Reuters*, 25 January 2019, https://www.reuters.com/.

7. Ellen Loanes, "These Are the Countries Where Russia's Shadowy Wagner Group Mercenaries Operate," *Business Insider*, 19 November 2019, https://www.businessinsider.com/.

8. Neil Hauer, "Russia's Favorite Mercenaries," *The Atlantic*, 27 August 2018, https://www.theatlantic.com/.

9. Andrew Linder, "Russian Private Military Companies in Syria and Beyond," *CSIS's New Perspectives in Foreign Policy* 16, 17 October 2018, https://www.csis.org/.

10. Zheng Wang, *Never Forget National Humiliation* (New York: *Columbia University Press*, July 2012, http://cup.columbia.edu/.

11. Doug Livermore, "China's 'Three Warfares' In Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, 25 March 2018, https://georgetownsecuritystudiesreview.org/.

12. Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, 28 January 2020, https://www.cfr.org/.

13. Eric Rosenbaum, "1 in 5 Corporations say China has Stolen Their IP within the Last Year: CNBC CFO Survey," *CNBC*, 1 March 2019, https://www.cnbc.com/.

14. B. R. Myers, *The Cleanest Race: How North Koreans See Themselves—and Why it Matters* (Melville House: Brooklyn, NY, 2011), 83.

15. "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," *Department of Justice*, 6 September 2018, https://www.justice.gov/.

16. Michael Raska, "Information Warfare on the Korean Peninsula," 13 March 2013, https://www.aspistrategist.org.au/.

17. Farzan Sabet and Roozbeh Safshekan, "Soft War: A New Episode in the Old Conflict Between Iran and the United States," *Iran Media Program*, November 2013, https://global.asc.upenn.edu/, 4.

18. Emily Blout, "Iran's Soft War With the West: History, Myth, and Nationalism in the New Communications Age," *SAIS Review of International Affairs* 35, no. 2 (Summer–Fall 2015): 33–44, accessed 20 May 2020, https://muse.jhu.edu/.

19. Seth G. Jones, "The United States' Soft War with Iran," *CSIS Briefs*, 11 June 2019, https://www.csis.org/.

20. Kate O'Flaherty, "The Iran Cyber Warfare Threat: Everything You Need to Know," *Forbes*, 6 January 2020, https://www.forbes.com/.

21. Alexandra A. Siegel and Joshua A. Tucker, "The Islamic State's Information Warfare: Measuring the Success of ISIS's Online Strategy," *NYU Scholars*, 2018, https://nyuscholars.nyu.edu/.

22. Robert J. Bunker and Pamela L. Bunker, Radical Islamist English-Language Online Magazines: Research Guide, Strategic Insights, and Policy Response (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, August 2018), https://publications.armywarcollege.edu/, xiii.

23. Bradford Burris, "Countering ISIL's Digital Caliphate: An Alternative Model," *Small Wars Journal*, 16 June 2017, https://smallwarsjournal.com/.

24. Office of the Chairman of the Joint Chiefs of Staff, "DOD Dictionary of Military and Associated Terms," Joint Chiefs of Staff (JCS), June 2020, https://www.jcs.mil/.

25. Department of Defense (DOD), *Deterrence Operations Joint Operating Concept* (Washington, DC: JCS, December 2006), https://www.jcs.mil/, 5.

26. Yale Law School, "Monroe Doctrine; December 2 1823," The Avalon Project: Documents in Law, History and Diplomacy, 2008, https://avalon.law.yale.edu/. See also James Polk, "State of the Union Address: James Polk (December 2, 1845)," 11 February 2017, https://www.infoplease.com/.

27. Ernest W. Lefevre, "The Sturdy Child of Terror," *Foreign Affairs*, 1 July 1999, https://eppc.org/.

28. "State of the Union; Transcript of President's State of the Union Message to the Nation," *New York Times*, 30 January 1991, https://www.nytimes.com/.

29. Paula Gottlieb, "Aristotle on Non-Contradiction," *Stanford Encyclopedia of Philosophy*, 6 March 2019, https://plato.stanford.edu/.

30. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*.

31. David P. Barash, "Nuclear Deterrence Is a Myth. And a Lethal One at That," *The Guardian*, 14 January 2018, https://www.theguardian.com/.

32. "Joint Publication 1, *Doctrine for the Armed Forces of the United States*, JCS, 12 July 2017, https://www.jcs.mil/.

33. Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington, DC: Georgetown University Press, 2019), 154, 2.

34. Bob Work, "Remarks by Deputy Secretary Work on Third Offset Strategy," DOD, 28 April 2016, https://www.defense.gov/.

35. Robert Farley, "What Scares China's Military: The 1991 Gulf War," *National Interest*, 24 November 2014, https://nationalinterest.org/. See also David Vergun, "DOD Comptroller: Overmatch Against China, Russia Critical," DOD, 10 April 2019, https://www.defense.gov/.

36. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 2011), 21.

37. DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018, https://dod.defense.gov/, 1.

38. Gen Charles Q. Brown Jr., "Accelerate Change or Lose," *US Air Force*, August 2020, https://www.af.mil/, 3.

39. Gen David G. Perkins, USA, "Multi-Domain Battle: The Advent of Twenty-First Century War," *Military Review*, November–December 2017, https://www.armyupress.army.mil/, 10–11.

40. Mark Pomerleau, "What the New 16th Air Force Means for Information Warfare," 13 October 2019, https://www.c4isrnet.com/.

41. US Africa Command Public Affairs, "Russia and the Wagner Group Continue to be Involved in Ground, Air Operations in Libya," *US Africa Command*, 24 July 2020, https://www.africom.mil/.

42. Barry Watts, "Countering Enemy 'Informationized Operations' in Peace and War," *Center for Strategic Budgetary Assessments*, 2013, https://www.esd.whs.mil/, 2.

43. Air Combat Command Public Affairs, "ACC Announces 24th and 25th NAF Merger," 5 April 2019, https://www.af.mil/.

44. "We Shall Fight on the Beaches," International Churchill Society, accessed 21 May 2020, https://winstonchurchill.org/.

VIEW

The Spectrum of Cyber Attack

Maj David Musielewicz, USAF

Introduction

Despite the extensive high-level guidance given by America's senior leaders in cyberspace, the risk of strategic failure and wasted resources remains high in offensive cyberspace operations. Former Secretary of Defense Ash Carter reflected on these failures in his description of countering the Islamic State of Iraq and Syria (ISIS) from 2015–17: "I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques. . . In short, none of our agencies showed very well in the cyber fight."[1]

This failure is due to the broad gap in the understanding of how leaders should pursue strategic objectives and goals at the tactical level. Although the Department of Defense most recently requested $3.7 billion for 2020 offensive cyberspace operations alone,[2] a clear, executable cyber attack framework that allows commanders to achieve senior leader visions does not currently exist. How can commanders reliably achieve the visions put forth by senior leaders given such a gap? I propose the following operational framework that bridges this gap and lays a foundation for the seamless pairing of tactical tasks and effects with desired strategic objectives.

If the United States is to have a distinct military advantage over its enemies, it must aggressively stay ahead of other nations in cyberspace through a framework at the operational level that offers speed and flexibility, while also succinctly connecting strategic guidance to tactical employment. A seamless flow from the strategic to tactical level will enable the alignment of action plans with overarching strategic goals throughout all echelons of cyberspace.

In the following sections, I draw on the previous decade of historical and currently active cyberwarfare alongside my 10 years of experience executing offensive cyberspace operations to frame attacks into a series of five levels that I collectively refer to as the "Spectrum of Cyber Attack." Each section defines and describes a particular level, provides real-world examples, and then explores the costs and benefits of conducting such attacks. A condensed depiction of these tradeoffs between cyber-attack levels is then estimated and summarized in the table. Finally, I propose future areas for consideration alongside the overall benefits of employing this framework throughout the various levels of leadership.

The Framework

By understanding the various attacks at each level within the spectrum, leaders and planners at the operational level will be better positioned to pursue objectives, describe expected end-states, and express various tradeoffs between methods. This will allow for the proper allocations of time, resources, and effort toward a particular objective. Ultimately, commanders will be able to present a menu of options for achieving strategic goals, all with varying levels of risk, reward, and resource commitment.

Throughout the brief history of cyberwarfare, actors at all levels have performed a wide range of attacks. Despite individual differences, these attacks can be arranged into five categories or levels that build upon one another to form a spectrum: Network Denial, Enterprise Denial, Enterprise Manipulation, Mission Denial, and Mission Manipulation.

The term *level* is best suited because of the compounding factor that exists between different attacks as they become more sophisticated. Once an actor can execute an attack at a higher level, they can also execute attacks at the lower levels. Conversely, conducting a denial attack at a lower level will likely cut off access to the systems required for higher-level attacks.

The following sections categorize these levels based on the estimated time required to execute an attack, their cost, their likelihood of success, how long they affect an organization, and their overall impact. In cyber warfare, almost all time is spent on gaining access to a particular system or systems crucial to the desired attack, while the time to execute the attack is negligible. Similarly, the policies and procedures to gain the appropriate approvals to conduct various attacks vary widely between organizations. Therefore, the time frames discussed throughout this article only refer to the operational time required to gain the requisite access, not the time required to initiate the attack or for various policies and processes.

The "Spectrum of Cyber Attack" incorporates the definition of denial from Joint Publication (JP) 3-12, *Cyberspace Operations*, "to prevent access to, operation of, or availability of a target function"[3] as the foundation for the three levels designated as denial attacks: Network Denial, Enterprise Denial, and Mission Denial. The spectrum builds upon JP 3-12's definition of manipulation, "controls or changes. . . to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification and other similar techniques,"[4] for the remaining levels designated as manipulation attacks: Enterprise Manipulation and Mission Manipulation. In this definition, *physical* simply refers to the fact that manipulation effects have an impact outside of cyberspace. This definition not only refers to the physical systems themselves, but also the cognitive layer, or users, of those systems.

This describes manipulating a system to in-turn manipulate or drive an effect in the human element. Manipulation attacks require a more complete understanding of the systems involved along with deeper, more intrusive network access. This knowledge and access are required to successfully manipulate, deceive, or otherwise influence the behavior of users within a target organization.

Level 1: Network Denial

Definition. A cyber attack that prevents a network from communicating with external networks

Description. The first level of attack is the most simple to conduct, difficult to stop, and thus commonly used. Level 1, Network Denial, targets only the transmission of information, not the actual information itself.

These attacks may affect only a part of the network or the network in its entirety. They can be accomplished through several different methods, many of which are exceedingly difficult for the victim to stop. Level 1 attacks primarily differ from other levels in that they affect the target's ability to interact with other organizations while internal processes are largely unaffected.

Examples. A simple example of Network Denial is characterized by an attacker that logs into a router at the border of an organization's network and stops it from transferring data. This example results in the blocking of all traffic on a network and isolates the target organization, temporarily preventing it from transmitting any information in or out using computer networks. This type of network isolation degrades the operations of any organization but only as long as the target is unable to restore proper functionality.

More advanced level 1 attacks require national-level resources or access to central backbones of the internet. These include Border Gateway Protocol hijacking, Domain Name Server hijacking, and large-scale Distributed Denial of Service, all of which have been used by either Russia, Iran, or China.[5] These attacks take advantage of the fundamental trust that the internet is built on, giving them the added benefit that there is very little a victim can do to stop them, and they are always at the disposal of a nation.

Tradeoffs. Network Denial attacks are conceptually simple to execute but only provide temporary paralysis of a target's operations. Fewer moving pieces at the technical level results in the highest chance for success compared to all other levels and requires far less knowledge about the target. New targets can be attacked within hours or days and require little preparation. The trade-off, however, is that level 1 attacks draw significant attention and are quick to diagnose. Overall, level 1 attacks require less time, less funding, and thus less commitment, yet they

are only expected to disable an organization for hours to days depending on the sophistication of the target's personnel.

Level 2: Enterprise Denial

Definition. A cyber attack that denies an organization's users access to their data

Description. The next level of cyber attack also disables an organization, but in a manner that inhibits the daily activities of end-users. The term *enterprise* is used to describe the systems and applications users rely on to perform day-to-day tasks. Examples of daily activities affected by level 2 attacks include the ability to log into computers, send e-mail, and alter documents. Level 2 attacks differ from level 1, Network Denial, in that they specifically disrupt information that an organization's users interact with directly.

Examples. The most common example of a level 2 attack is ransom malware, or "ransomware," currently in vogue with cybercriminals. Ransomware does not need to know anything about an organization before executing its core objective, to deny users access to their data by encrypting it. The files that become encrypted are critical to the system users as the malicious software attacks all files, historical records, activity records, and any others used to carry out daily tasks and company function. This is precisely why it is so devastating for companies hit by such attacks.

The most destructive level 2 attack to date has been the "NotPetya" ransomware that caused an estimated $10 billion in damages worldwide in 2017. As an example of the financial impact caused by NotPetya, the international shipping company Maersk alone suffered $300 million in damages and experienced a complete operational shut down for almost a week. This level of disaster is not unique to Maersk,[6] or even NotPetya itself. "WannaCry," "SamSam," and "Ryuk" are all well-documented ransomware attacks dating back to 2017 that inflicted millions in financial costs and achieved wide-scale operational impacts across numerous organizations.[7]

Tradeoffs. Level 2 attacks are likely to cost more financially than any other cyber attack, purely based on the scope and number of systems they affect. Similar to level 1, level 2 attacks require very little target knowledge, and thus, require less time and monetary investment than other levels. However, the likelihood of success of level 2 attacks is also less than that of level 1 attacks due to the deeper network access required. Additionally, the most damaging level 2 attacks to-date only managed to take organizations offline for a few days despite the severe financial costs, and all operations were restored in a manner of weeks.

Level 3: Enterprise Manipulation

Definition. A cyber attack that manipulates the decision-making of an organization's users without being detected

Description. Enterprise Manipulation is the first level on the spectrum that tailors more toward affecting the behavior of the adversary than removing their ability to operate. These attacks target the same computer systems as level 2, Enterprise Denial, attacks but utilize a deeper understanding of the organization to influence or corrupt, but not deny, common organizational processes. Further, a key objective in executing a level 3 attack is to do so without the user being aware of the attack. This is the key distinction between level 3 and the first two levels.

Level 3 attacks must be performed in a manner that is not predictable nor widespread throughout the target organization. Enterprise users have been conditioned over time to be mistrusting of computers and software due to confusing interfaces, technical user manuals, overall complexity, and frequent data loss. By introducing outside gremlins into the systems, end-users can further lose confidence in their ability to effectively perform tasks, thereby leading to loss in productivity and organizational effectiveness.

Examples. Although data manipulation has only started to be openly discussed in the past few years,[8] it is easy to envision the potential chaos that can result from such attacks and has captured the imagination of television producers in series such as "Mr. Robot."[9] These attacks can be as simple as removing key e-mails, locking particular user accounts, or corrupting vital user files. More robust and potentially far-reaching attacks can be catastrophic, such as manipulating financial or human resource data.

According to *Forbes*, the manipulation of financial data is already extensively practiced by North Korean hackers. North Korea has stolen a staggering $2 billion in 35 compromises across 17 nations.[10] For example, North Korea drained $498K from the city of Tallahassee by manipulating payroll data.[11] These attacks were designed to obtain funds rather than impose crippling costs on the underlying organizations, yet the devastating impact to the organizations were the same.

Tradeoffs. Enterprise Manipulation attacks strike at the psyche of an organization with the aim of crippling its effectiveness for a prolonged period of time. Levels 1 and 2 cause overt disruptions resulting in temporary outages, but level 3 attacks can hinder an organization for an indefinite period of time. These attacks require a nearly identical preparation time as level 2 but have a much lower chance of success and less quantifiable results. Level 3 attacks also cost more to execute because they must use more sophisticated tools to remain undetected in the target network. Level 3 attacks will not likely impose costs similar to the other levels, but

they allow attackers to remain within the network undetected while eroding the productivity of an organization.

Level 3 attacks also provide the ability to engage a target without the increased risks of retaliation or escalation because of their inherent stealth and plausible deniability. As long as level 3 attacks remain hidden, they allow the perpetrator to develop level 4 and level 5 attacks, all while the target simultaneously suffers negative impacts on efficiency and productivity.

Level 4: Mission Denial

Definition. A cyber attack that specifically prevents the operation of processes or systems critical to an organization's mission

Description. The final two levels of the Spectrum of Cyber Attack focus solely on the chain of systems and processes that are essential to an organization carrying out its core mission. This focus may be the destruction of mission-critical data or even—in very specific scenarios—the physical destruction of hardware through industrial control system manipulation. The precision of these attacks is what specifically distinguishes level 4, Mission Denial, from level 2, Enterprise Denial.

Example. The 2015 Russian attack on the Ukraine power grid is a prime example of a level 4 cyber attack. During this attack, Russia gained critical access to three primary Ukrainian power companies undetected. Once inside the networks, the malicious actors immediately targeted the systems used by internal operators to control the generation of power. The actors surveilled the system operators long enough to learn which interfaces were used to control the power generators. Once known, the attackers systematically shut the generators down and disabled remote access to the controlling computers.[12] By preventing the power generator operators from remotely bringing the systems back online, technicians were required to physically travel and manually restart each generator, a process that took six hours to complete.[13]

What makes this example a level 4 attack instead of a level 2 is that the actors were specifically targeting those systems that were essential to the organization executing its core mission—generating power. If these same actions were conducted against systems not vital to this mission, they would be classified as a level 2 attack.

Tradeoffs. From an attacker's perspective, level 4 attacks are much more predictable than level 2 because of their precise nature. These attacks are far more likely to create the specific effect desired. Reducing the scope of an attack and executing with precision allows the attacker to tailor to specific strategic objectives and execute with a higher level of certainty. In contrast, level 2, Enterprise Denial, has the potential to prevent an organization from accomplishing its pri-

mary mission, but only as a byproduct of the primary attack. It is easier for a victim to restore mission-critical functions following a level 2 attack because of the universal aspect of level 2 attacks versus the subtlety required for level 4. Level 2 attacks are far more common and less sophisticated, making them more likely to be anticipated and mitigated by network defenders.

Level 4 attacks require notably longer time commitments than levels 1, 2, and 3. This is due to the in-depth understanding required to learn the specifics of how an organization conducts its mission and the time required to maneuver to those systems that enable that mission. These longer time commitments naturally cause the overall cost of operations to go up. The longer an actor must remain in a network, the more sophisticated their tools must be to stay undetected. Once a level 4 attack is executed, it will quickly be discovered by network defenders and the remedy will likely be straightforward. The effective downtime of the organization relies heavily on the extent of any physical damage and is further influenced by the scarcity of any specialized hardware required.

Level 5: Mission Manipulation

Definition. A cyber attack that specifically manipulates the systems or processes critical to an organization's mission without being detected

Description. Mission Manipulation is the most sophisticated and strategically complex cyber attack within the spectrum. Mission Manipulation allows for the repeated, sustained disruption of the fundamental mission of an organization. Level 5 attacks are identical to level 4 except for the critical fact that they are executed without being detected. This is a small distinction but is exceptionally difficult to achieve.

Example. The destruction of mission-critical systems and the manipulation required to hide those actions has only been demonstrated by one publicly disclosed cyber attack to date: Stuxnet. Extensively documented, Stuxnet is known for the physical destruction it inflicted on Iranian centrifuges from April 2009–June 2010.[14] Yet, the true brilliance of Stuxnet was its skillful deception of the end-users of these systems. Stuxnet systematically destroyed these mission-critical centrifuges while at the same time manipulating the monitoring components to tell the engineers they were functioning properly.

Because of the criticality of these centrifuges, the paired destruction and deception of Stuxnet disrupted the organization's ability to perform its primary mission and set back Iran's nuclear program a minimum of two years.[15] The attack exacerbated financial burdens and according to a report by the Center for Security Studies, "likely culminated in an overall feeling of insecurity throughout Iranian society."[16] Even after the discovery of Stuxnet, Iran was not able to fully trust their

systems—not knowing whether a failure was generated by human error or the actions of malicious code lurking in their systems.

Tradeoffs. Level 5 attacks require substantially more resources than any other level, both in time and human capital. Mission Manipulation is expected to require a combination of customized tools, in-depth knowledge, sophisticated cyber expertise, specialized engineering knowledge, and significant amounts of time. It requires time to gain network access, time to harvest information, time to develop tools, time to maneuver within the network, and time to execute. It was speculated that Stuxnet required the combined efforts of Israel and the United States[17]—two of the most technologically sophisticated nations in the world—a minimum of three years of preparation, a year of continuous execution, and an estimated $100 million dollars.[18]

The target knowledge, commitment, and technical expertise required to execute attacks at level 5 demands real-time development as the exact configurations and nuances of mission systems are almost impossible to know before accessing them. The skills and tools for such specialized or indigenous mission systems may be extremely hard to find, or may not exist, requiring them to be built from the ground up.

In spite of these heavy constraints, a level 5 attack has the ability to cause massive high-level impacts that rival the sophistication of any operation in the other warfare domains. It can single-handedly achieve strategic objectives through non-kinetic means, and importantly, allow for plausible deniability that reduces the risk of retaliation and conflict escalation. As seen in the Stuxnet example, the culmination of such high levels of investment can produce powerful effects that last for years.

Conclusions and Expansion

By defining the attributes and characteristics of attacks at each level within the Spectrum of Cyber Attack decision-makers are better positioned to understand and pursue strategic objectives. Strategic guidance can be succinctly delivered, and tactical tasks can be determined more rapidly. Moreover, this operational framework presents a clear roadmap for building out a menu of options that incrementally increases the required resources and effectiveness when engaging a target. Although each described level presented several examples, the creative opportunities within or between levels are largely unlimited—especially as this field of knowledge continues to expand.

While this framework was developed with offensive cyberspace operations in mind, there may also be ways it can be used in defensive cyberspace operations to interpret the intent and resources of an adversary's attack. The framework may

allow defenders to quickly triage the holistic threat to a network, not just the immediate threat to a single host, and allocate resources accordingly.

Additionally, operations using this framework could greatly benefit from a more thorough exploration of the possible psychological effects that could result from cyber attacks at each level. Since cyber operations are nonkinetic in nature, attacks leveraging psychological operations—particularly level 3 attacks—could have significant impacts on an adversary in ways kinetic attacks cannot. Using this framework as a prism, a focused examination of combined arms that uses both psychological and cyber operations could yield even more effective methods for influencing an adversary.

Overall, the Spectrum of Cyber Attack is a straightforward framework that works to bridge the gap between strategic doctrine and the appropriate tactical tasks pursued through offensive cyberspace operations. As this framework is adopted and further refined, the end-result will allow commanders and planners to pair desired end-states with the proper actions based on resource requirements and constraints. By understanding strategic objectives and aligning them with a given cyber-attack level, commanders can more effectively prosecute targets, produce desired strategic outcomes, and uniquely contribute to winning our nation's conflicts. ✪

Table. Estimated tradeoffs between cyber-attack levels

Level	Cost to execute	Preparation time	Likelihood of success	Impact duration	Severity of impact
1	$1K+	Days	High	Days	Low
2	$10K+	Weeks	Medium	Weeks	Medium
3	$50K+	Weeks	Medium	Years	Low
4	$100K+	Months	Low	Weeks	Medium
5	$1M+	Years	Low	Years	High

Key: K = thousand, M = Million

Maj David Musielewicz, USAF

Major Musielewicz (BS, USAFA; MS, Georgia Institute of Technology) is a combat mission team lead for US Cyber Command, Lackland AFB, Texas. With more than 300 missions and 2,100 hours on offensive cyber platforms, he previously served as a cyber-attack operator at the National Security Agency, Fort Meade, Maryland.

Notes

1. Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, October 2017, https://www.belfercenter.org/.

2. Mark Pomerleau, "What's in the $9.6B Cyber Budget Request?" *Fifth Domain*, 14 March 2019, https://www.fifthdomain.com/.

3. Joint Publication (JP) 3-12, Cyberspace Operations, 8 June 2018, II-7, https://www.jcs.mil/.

4. JP 3-12, *Cyberspace Operations*.

5. Justin Sherman, "Hijacking the Internet Is Far Too Easy," *Slate Magazine*, 16 November 2018, https://slate.com/; Brian Krebs, "A Deep Dive on the Recent Widespread DNS Hijacking Attacks," *Krebs on Security*, 18 February 2019, https://krebsonsecurity.com/; and Jon Porter, "Telegram Blames China for 'Powerful DDoS Attack' during Hong Kong Protests," *The Verge*, 13 June 2019, https://www.theverge.com/.

6. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired Magazine*, 22 August 2018, https://www.wired.com/.

7. Phil Muncaster, "WannaCry Cost NHS £92 Million," *Infosecurity Magazine*, 15 October 2018, https://www.infosecurity-magazine.com/; Zack Whittaker, "Atlanta Projected to Spend at Least $2.6 Million on Ransomware Recovery," *ZDNet*, 23 April 2018, https://www.zdnet.com/; and Sam Dean, "What Is Ryuk, the Malware Believed to Have Hit the Los Angeles Times?," *Los Angeles Times*, 1 January 2019, https://www.latimes.com/.

8. Sean Lyngaas, "Former NSA Chief: Data Manipulation an 'Emerging Art of War,'" *FCW: The Business of Federal Technology*, 22 October 2015, https://fcw.com/.

9. Kayleena Pierce-Bohen, "10 Technological Threats in Mr. Robot That Are Actually Real," *Screenrant*, 27 May 2019, https://screenrant.com/.

10. Kate O'Flaherty, "North Korean Hackers' $2 Billion Heist Is 'Funding WMD Programs,'" *Forbes Magazine*, 7 August 2019, https://www.forbes.com/.

11. Karl Etters, "Almost $500,000 Swiped in City of Tallahassee Payroll Hack," *Tallahassee Democrat*, 5 April 2019, https://www.tallahassee.com/.

12. Robert M. Lee, Michael J. Assante, and Tim Conway, "TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS*, 18 March 2016, https://ics.sans.org/.

13. Darren Pauli, "Malware 'Clearly' behind Ukraine Power Outage, SANS Utility Expert Says," *The Register*, 15 January 2016, https://www.theregister.co.uk/.

14. Jim Finkle, "Factbox: Cyber Warfare Expert's Timeline for Iran Attack," Martin Howell, ed., *Thomson Reuters*, 2 December 2011, https://www.reuters.com/.

15. Yaakov Katz, "'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years,'" *Jerusalem Post*, 15 December 2010, https://www.jpost.com/.

16. Marie Baezner and Patrice Robin, "Stuxnet," *ResearchGate, ETH Zurich*, 15 February 2018, https://www.researchgate.net/.

17. William J. Broad, John Markoff, and David E Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, https://www.nytimes.com/.

18. Finkle, "Factbox: Cyber Warfare Expert"; Dennis Fisher, "Cost of Doing APT Business Dropping," *Threatpost*, 6 February 2014, https://threatpost.com/.

VIEW

Information Warfare and Joint All-Domain Operations

A Primer for Integrating and Prioritizing Data Requirements

Lt Col Bradley M. Pirolo, USAF

Introduction

The US Air Force (USAF) is at risk of losing the next conflict if we do not change, as noted by Gen Charles Q. Brown, the 22nd USAF chief of staff, within weeks of taking the reins via his "Accelerate Change or Lose" charge. This risk is at least mainly because there is currently no effective, integrated flow of information warfare (IW) data products and services into command and control (C2) systems to enable enhanced tactical and operational war-fighter and decision-maker situational awareness. The USAF and joint services remain constrained to legacy, industrial era, and static databases for all the data, intelligence products, and services that the various tenets of IW provide—if the services even possess any consolidation of such data at all. These datasets and databases must become available to the Advanced Battle Management System (ABMS) in near real-time to enable our USAF, joint, and allied force success in conducting joint all-domain operations (JADO) in future peacetime competition and combat actions across the global commons. We would not allow our friends to go into a cage fight blindfolded, so why would the IW component of the USAF enable our service, sister services, and allied partners to enter any nation versus nation competition or conflict blind? We must work promptly to ensure the integration of IW into ABMS to integrate our ability to operate from that mosaic of information down to the tactical level and enable "uncomfortable delegation" of C2 to that 8-ship flight lead over the South China Sea. Victory is not assured in all conflict and competition, but we can certainly increase our chances of future victory by planning and organizing proactively.

The *National Defense Strategy* of 2018 prominently noted: "inter-state strategic competition, not terrorism, is now the primary concern in US national security."[1] Much has changed since that strategy document's release, including the defense secretaries and the paradigms under which we as officers, noncommissioned officers, and civilians acting as leaders, planners, and staffers operate to organize, train, and equip the USAF. That change has been immensely sufficient in enabling the USAF to adapt to "the increasingly complex security environment. . . defined by rapid technological changes [and] challenges from adversaries in every operat-

ing domain," such that we prioritize that it is "most important to field a lethal, resilient, and rapidly adapting Joint Force."[2] To that end, the USAF now finds itself, along with the joint services, wrestling with how to adapt to an era where freedom of maneuver and the ability to mass forces is again fundamentally at risk, in a way that it has fundamentally not been since the Fulda Gap scenarios of the 1980s Cold War competition with the Soviet Union.

The Pacing Threat of Peer Adversaries

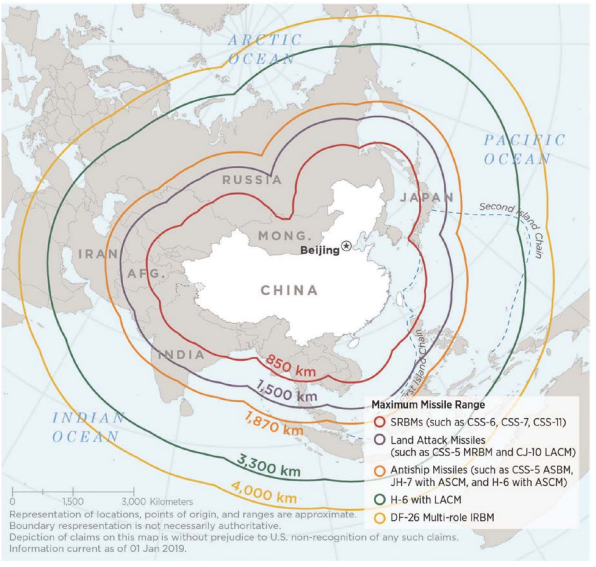


Figure 1. Chinese Conventional Strike Capabilities

Source: *OSD Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 45

The reason for this struggle, of course, stems from the efforts of our peer adversaries, described in clear detail within the *National Defense Strategy* of 2018 as including the People's Republic of China and the Russian Federation to develop, field, and proliferate technologically advanced anti-access/area-denial weapons systems. They have done this to limit any third party's, in essence the United States', ability to intervene in their national objectives relative to nation-state engagements.[3] These advanced systems and their C2 enterprise collectively present joint and allied forces with a significantly contested and degraded operations space. It is well characterized that both China and Russia have developed double-digit surface-to-air missile systems and advanced fifth-generation fighters that they placed along borders, key C2 hubs, and the littoral to prohibit air interdiction. The Chinese People's Liberation Army Rocket Force has fielded advanced and mobile, terminally guided antiship ballistic missiles that force US Navy car-

rier strike groups to operate at extended ranges from their targets. Both the Democratic People's Republic of Korea and China field mobile and advanced intermediate-range ballistic missiles such as the DF-26, potentially armed with nuclear weapons that place key joint force marshaling locations and fixed bases such as Anderson AB, Yokosuka Naval Air Station, or the III MEF Headquarters on Okinawa at risk.[4] All of that says nothing of the nonkinetic concerns that a peer adversary such as the Russian Federation presents via the use of combined cyber and information operations to enable the advance of irregular forces to infiltrate and commandeer an allied nation via hybrid warfare. Everywhere, the threat to the USAF's freedom of maneuver is real and clear. Never has it been more accurate than now that our adversaries are strategically targeting our power projection centers of gravity and developing the means to defeat us through their dismemberment of *schwerpunkt* (assessed "critical focal points" in the form of static C2 centers at the operational- and theater-level of warfare).

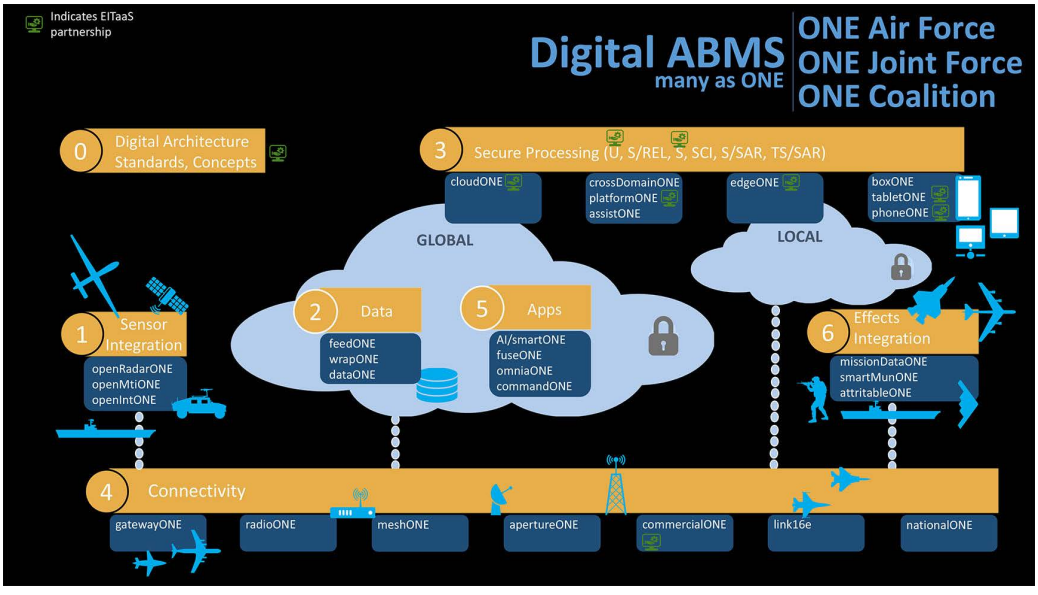


Figure 2. ABMS Overview

Source: CSAF—Wing Commanders Call, JADC2 & ABMS, 17 September 2020, 7.

Joint All-Domain Operations and Command and Control

As the post-COVID-19 world begins to recalibrate itself to the previously emerging great-power competition already well underway at the pandemic's outset, the USAF and its joint service peers will charge full speed ahead with implementing doctrinal joint all-domain command and control (JADC2) to enable JADO. As articulated by USAF Gen Paul J. Selva, as vice chairman of the Joint

Chiefs of Staff, JADC2 aims to secure resilient C2 and battlespace awareness sufficient to enable and integrate fires across the variety of disparate shooters and sensors operated across a joint or combined task force. It intends to reconceptualize the headquarters elements such as an air operations center or tactical operations center naturally dislocated from the forward edge action. JADC2 aims to empower tactical commanders immersed in high-intensity forward, tactical-edge combat with the same SA and empowered C2 decision-making that would previously have been reserved for what are now at-risk as *schwerpunkt*. This concept enables force management that is responsive to, even out in front of, enemy or adversary generated effects, decision-making, and maneuvering. JADC2 seeks to be executable even when networks are disconnected, reduced in bandwidth, or intermittent, as can and should be expected when fighting or competing in earnest with adversaries in the twenty-first century. The end goal of all this connectivity and pristine situational awareness will be friendly forces' ability to synchronize the prosecution of thousands of potential targets across a federated resource set of the combat arms inherent to the task force and across domains.[5]

This situation only happens via the stand-up and rollout of ABMS. ABMS represents a $3.3 billion investment through fiscal year 2025 by the USAF and intends to serve as a data-integrating, command-decision enabler that spurs the Find, Fix, Target, Track, Engage and Assess process. The intent is that ABMS will aid active battlespaces and within those murkier, harder-to-define scenarios and environments that we as a nation and the USAF will find ourselves increasingly operating (i.e., peacetime competition).[6] In places such as the Kuril Islands, the waters of the South China Sea, the airspace of the Black Sea, the outskirts of Kaliningrad, and all around the Baltic, America, and her allies will assuredly be forced to proactively confront the advances of our peer adversaries in ways short of war. With those adversaries' intentions laid bare more than ever before, the only way to effectively confront those ambitions now is via effectively interlaced joint and combined (read *allied*) force approaches.

Per reporting, ABMS will be driven by artificial intelligence and employ machine learning but, more importantly, will integrate into seven categories of actions or applications. These categories include digital architectures, standards and concept development; sensor integration; multidomain data management; multidomain secure processing; multidomain connectivity; multidomain applications; and effects integrations. These effect integrations include smart munitions, attritable aircraft, and the rapid reprogramming of electric warfare mission data files in near real-time.[7] What do all of these advertised elements of ABMS have in common? A distinct reliance upon IW and data or intelligence derived from the same to function at peak performance to support JADO.

The Prioritization and Integration of Information Warfare

To achieve that peak performance, we need ABMS, and it will, in turn, require critical data provided via the tenets of IW. This requirement includes critical intelligence derived from observations of and operations within cyberspace, electronic warfare and the electromagnetic spectrum, and intelligence derived from information and intelligence, surveillance, and reconnaissance (ISR) operations. One subset of data that will be critical to interlink within ABMS—in which the Air Force Life Cycle Management Center is beginning to evaluate for integration—is intelligence mission data (IMD). All too often an afterthought in consideration, as was the case in the Technology Maturation and Risk Reduction phase of the F-35 Joint Strike Fighter program's acquisition, IMD represents a crucial component to both the ability of ABMS to function successfully and to provide situational awareness to operational commanders and tacticians executing their mission orders and taskings. IMD includes order of battle, characteristics and performance, geospatial intelligence, and electronic warfare integrated reprogramming data and signatures data. The requirements for IMD are documented early in a weapon system program's development and are captured within an associated Life-Cycle Mission Data Plan. When IMD is integrated, and accurate, joint and allied forces avoid fratricide and hone their battlespace awareness through combat ID. This integration enables those forces to seize the high ground, hold adversary targets at risk, and win the day. Compared with ABMS, IMD receives a USAF budget slice of barely $40M annually, representing an outsized potential to affect JADC2 positively.

IMD is certainly not alone in its criticality to fielding a functioning ABMS and enabling the joint and allied force to execute to JADO. Cyberspace operations, information operations, and the intelligence-derived from ISR operations must also be able to integrate within ABMS so as to update the JADC2 reality presented to tactical decision-makers. Each component of IW can contribute a myriad of datasets to the ABMS mosaic. Within IW, cyberspace operations provide the ability to defend the ABMS network itself and present a matrix of cyber vulnerabilities possessed by the adversary for exploitation and targeting. Information operations would enable commanders to safeguard joint task force feints from the real surprise dynamic force deployments intended to throw the adversary back on their heels, representing datasets that must be available to ABMS. ISR operations provide the ability to yield critical intelligence on mobile SAM and theater ballistic missiles repositioning to enable interdicting joint fires; this intelligence must quickly transition onto ABMS to enable shooter decisions. Across the board, IW has critical data to offer, ensuring the mosaic is its most complete and accurate. However, that data must be integrated and early to enable ABMS to be successful.

Recommendations

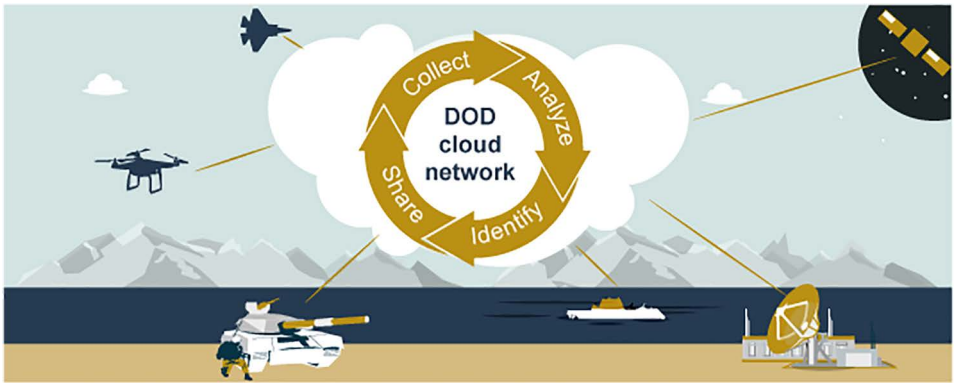


Figure 3. Government Accountability Office ABMS Analysis

Source: Action is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System, US Government Accountability Office (GAO-20-389), 16 April 2020.

In conclusion, we can delay modernization no longer. Our adversaries, like China, simply will not allow for it. The Defense Intelligence Agency has initiated an effort to transition static, foundational intelligence databases like the Modernized Integrated Database (MIDB) into a worldwide web-like application in the form of a machine-assisted rapid-repository system (MARS). This system represents an excellent first step in transforming the environment for foundational military intelligence and interactions with same.[8] However, such efforts are insufficient to actualize the integration of decision-enhancing IW-derived intelligence data in JADC2 constructs via mechanisms like ABMS. Neither do such efforts comprise threat warning, collection management, and targeting intelligence equities necessary to create the most robust picture for war fighters. What is called for is promulgation and federation of all IW-produced data and intelligence, through a cloud-based federation enabled by automation and machine learning algorithms, onto the ABMS cloud and into cockpits. This shared intelligence, tagged and integrated with tactical sensor data and multifunction displays, will enable true decision advantage for the USAF, joint services, and our allies, critically enabling them to reinvigorate intelligence databases with their combat mission's findings and observations. The following concrete measures can accomplish this:

- Establish clear requirements for all tenets of IW products and services in JADC2 "Concept Required Capabilities."
- Integrate existing intelligence and IW databases within the ABMS Cloud.
- Develop and implement security protocols and cross-domain solutions to enable IW and intelligence data transfers to and through ABMS, and for

sensor and platform-derived data in the opposite direction and into intelligence databases.

- Assure appropriate data labeling and tagging to sources of data.
- Service-wide training to establish tactics, techniques, and procedures for IW, intelligence, and sensor data utilization and transfer.

Conclusion

Such a significant transformation affecting the IW enterprise, the role of the intelligence, and other provided data services for the joint war fighter will not occur overnight. It will require a significant paradigm shift in how producers, curators, and consumers of such data will conduct their relative operations and how the unit level integrates its combat mission results back into the intelligence community and IW enterprise. This task will not be easy and will require a joint approach, but American innovation must, can, and will win the day over Chinese reverse engineering—if senior leaders foster and guide that innovation into being. ✪

Lt Col Bradley M. Pirolo, USAF

Lieutenant Colonel Pirolo (BA, University of Florida; MSIR, Troy University) is the commander of the 57th Intelligence Squadron, an intelligence mission data production squadron at Joint Base San Antonio-Lackland, Texas. He is an intelligence weapons officer who has deployed in support of combat missions in Operation Iraqi Freedom, Operation Enduring Freedom, and Operation New Dawn. Lieutenant Colonel Pirolo previously served as the chief of the strategic intelligence, surveillance, and reconnaissance requirements division, Headquarters, Air Force Global Strike Command.

Notes

1. Department of Defense (DOD), *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, 2018), https://dod.defense.gov/.
2. DOD, *Summary of the 2019 National Defense Strategy*.
3. Office of the Secretary of Defense (OSD), "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2019," 2 May 2019, https://media.defense.gov/.
4. OSD, "Annual Report to Congress."
5. Lt Col Aaron Gibney, "Joint All-Domain Command & Control (JADC2) Campaign Plan–Planning Conference 27–29 August 2019-Outbrief," August 2019: 3–4.
6. Rachel S. Cohen, "Air Force Bets on ABMS Success in Fiscal 2021," *Air Force Magazine*, 11 February 2020, https://www.airforcemag.com/.
7. Cohen, "Air Force Bets on ABMS Success."
8. Defense Intelligence Agency (DIA), *Strategic Approach: Committed to Excellence in Defense of the Nation* (Washington, DC: DIA, September 2018) https://www.dia.mil/.

BOOK REVIEW

Military Strategy in the 21st Century: People, Connectivity, and Competition by Charles Cleveland, Benjamin Jensen, Susan Bryant, and Arnel David. Cambria Press, 2018, 238 pp.

Military Strategy in the 21st Century: People, Connectivity, and Competition is a strategy focusing on the development of the human domain and information warfare as it relates to the national and theater-level policy making. The text draws upon retired Army Lt Gen Charles Cleveland's distinguished Special Forces career and those of Benjamin Jenson, Susan Bryant, and Arnel David, all of whom are active or retired US Army officers with strategic planning backgrounds.

The central thesis for the book "outlines a new approach to thinking about military art rooted in increasing connectivity and define a new domain of competition, the human domain" (p. 4). Like similar strategy texts, this book looks at the evolving character of war and competition in the new century accepting that the nature of war remains the same. The book is admittedly biased toward ground operations but is well-researched, drawing from lessons learned documents from the US's recent conflicts across the Middle East. The authors have brought some salient points forward about conflicts that have evolved greatly, but which the US is still fighting.

In the chapter titled "Rusting Sword," the authors explored the decline of decisive conflict in the post-Cold War area. Drawing from empirical data, they argued that armed conflict has progressed to more nonvictory and less decisive outcomes than previous epochs. From the rise of the dispersion of information (away from the state to the broader populace) to the growth of intrastate conflict, there has been investment in blood and treasure with a limited return, resulting in a shift that "highlights both misalignment of strategic objectives and military objectives and a new character of war" (p. 89).

The chapter on information warfare was especially insightful. It started with a concise history of US information warfare efforts following World War II and into the Cold War. The outlining the shift in thinking away from human-based information warfare toward the network warfare concepts that developed in the 1990s. Additionally, it pays heed to the United States' twenty-first-century peer competitors, China and Russia—both their thinking and approach to the subject.

The authors continue with further discussions on the human domain and the global security network. They discuss a number of topics from the United States' penchant for attrition-based strategies post-Civil War to networks and strategy. This is a wide-ranging discussion that would benefit from further in-depth analysis and details to further tease out key points to the importance of humans to human conflict.

While this author does not see the "human domain" rise to the level of the conventionally accepted domains of land, sea, air, space, and cyberspace, it most certainly drives home the point that conflict is about the humans in competition, not just the weapons used to fight. For those planning and strategizing for the burgeoning great-power competition, *Military Strategy in the 21st Century* would be a worthy read to ensure that hard-fought lessons learned since World War II are not forgotten for the future.

Lt Col Benjamin L. Carroll, USAF

Air University Press

Call for Articles and Manuscripts

Joint All Domain Command and Control (JADC2)

Air University Press is soliciting manuscripts, journal articles, and short papers that focus on Joint All Domain Operations (JADO—see LeMay Doctrine Note 1-20). More specifically, Joint All Domain Command and Control (JADC2), is defined as "The art and science of decision making to rapidly translate decisions into action, leveraging capabilities across all domains and with mission partners to achieve operational and information advantage in both competition and conflict."

Products could be historical case studies, lessons learned from ongoing initiatives, or suggestions for future constructs. Length may vary from journal articles (typically under 15,000 words), papers (15,000-75,000 words), or full-length book manuscripts (over 75,000 words). Submit works to the Director of Air University Press. Digital submissions and inquiries are also welcome through our organizational email at AirUniversityPress@au.af.edu.